EUROPEAN STANDARD **prEN 50129**

NORME EUROPÉENNE

EUROPÄISCHE NORM December, 1999

ICS

Descriptors: Railway equipment, safety related systems, electronic components, safety integrity levels, safety requirements, safety acceptance, safety case

English version

Railway Applications : Safety related electronic systems for signalling

Applications aux chemins de fer: Systèmes électroniques de sécurité pour la signalisation

Eisenbahntechnik: Sicherheitsrelevante elektronische Systeme für Signaltechnik

This draft European Prestandard is submitted to CENELEC members for CENELEC enquiry.

It has been drawn up by SC 9XA of Technical Committee CENELEC TC 9X.

If this draft becomes a European Standard, CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national without any alteration.

This draft European Standard was established in English version only.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization

Comité Européen de Normalisation Électrotechnique

Europäisches Komitee für Electrotechnische Normung

Central Secretariat: rue de Stassart 35, B-1050 Brussels

Foreword

This draft European standard was prepared by the Subcommittee SC 9XA, communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways. It is submitted to CENELEC members for CENELEC enquiry.

The text incorporates the experience with ENV 50129, which validity ends at 30.6.2001.

Annexes designated “informative” are given for information only. In this prEN 50129, annexes D,E,F are informative.

The following dates are proposed:

latest date by which the existence of the EN has to be announced at national level	(doa) 2001-07-01
latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop) 2001-12-01
latest date by which the national standards conflicting with the EN have to be withdrawn	(dow) 2002-07-01

Table of content

Introduction

This document is the first European Standard defining requirements for the acceptance and approval of safety-related electronic systems in the railway signalling field. Until now only some differing national recommendations and general advice of the UIC (International Union of Railways) on this topic were in existence.

Safety-related electronic systems for signalling include hardware and software aspects. To install complete safety-related systems, both parts within the whole life-cycle of the system have to be taken into account. The requirements for safety-related hardware and for the overall system are defined in this standard. Other requirements are defined in associated CENELEC standards.

The aim of European railway authorities and European railway industry is to develop compatible railway systems based on common standards. Therefore cross-acceptance of Safety Approvals for sub-systems and equipment by the different national railway authorities is necessary. This document is the common European base for safety acceptance and approval of electronic systems for railway signalling applications.

Cross-acceptance is aimed at generic approval, not specific applications. Public procurement within the European Community concerning safety-related electronic systems for railway signalling applications will in future refer to this standard when it becomes an EN.

The standard consists of the main part (Sections 1 to 5) and annexes A, B, C, D, E and F. The requirements defined in the main part of the standard and in annexes A, B and C are normative, whilst annexes D, E and F are informative.

This standard is consistent with, and uses relevant sections of, EN 50126: "Railway Applications: The Specification and Demonstration of Dependability - Reliability, Availability, Maintainability and Safety (RAMS)". In particular, both standards are based on the system life-cycle.

Because this standard is concerned with the evidence to be presented for the acceptance of safety-related systems, it specifies those life-cycle activities which shall be completed before

the acceptance stage, followed by additional planned activities to be carried out after the acceptance stage. Safety justification for the whole of the life-cycle is therefore required.

This standard is concerned with what evidence is to be presented. Except where considered appropriate, it does not specify who should carry out the necessary work, since this may vary in different circumstances.

For safety-related systems which include programmable electronics, additional conditions for the software are defined in EN 50128: "Railway Applications: Software for Railway Control and Protection Systems".

Additional requirements for safety-related data communication are defined in EN 50159-1 and EN 50159-2.

1 Scope

This standard is applicable to safety-related electronic systems (including sub-systems and equipment) for railway signalling applications.

The scope of this standard, and its relationship with other CENELEC standards, are shown in figure 1.

This standard is intended to apply to all safety-related railway signalling systems/sub-system/equipment. However, the hazard analysis and risk assessment processes defined in EN 50126 and this standard are necessary for all railway signalling systems/sub-systems/equipment, in order to identify any safety requirements.If analysis reveals that no safety requirements exist (i.e.: that the situation is non-safety-related), and provided the conclusion is not revised as a consequence of later changes, this safety standard ceases to be applicable.

This standard applies to the specification, design, construction, installation, acceptance, operation, maintenance and modification/extension phases of complete systems, and also to individual sub-systems and equipment within the complete system. Annex C includes procedures relating to electronic hardware components.

This standard applies to generic sub-systems and equipment (both application-independent and those intended for a particular class of application), and also to systems/sub-systems/equipment for specific applications.

This standard is not applicable to existing systems/sub-systems/equipment (i.e. those which had already been accepted prior to the creation of this standard). However, as far as reasonably practicable, this standard should be applied to modifications and extensions to existing systems, sub-systems and equipment.

This standard is primarily applicable to systems/sub-systems/equipment which have been specifically designed and manufactured for railway signalling applications. It should also be applied, as far as reasonably practicable, to general-purpose or industrial equipment (e.g.: power supplies, modems, etc.), which is procured for use as part of a safety-related signalling system. As a minimum, evidence shall be provided in such cases to demonstrate:

either: that the equipment is not relied on for safety;

or: that the equipment can be relied on for those functions which relate to safety.

This standard is applicable to the functional safety of railway signalling systems. It is not intended to deal with the occupational health and safety of personnel; this subject is covered by other standards.

This standard is the sector specific interpretation of IEC 61508.

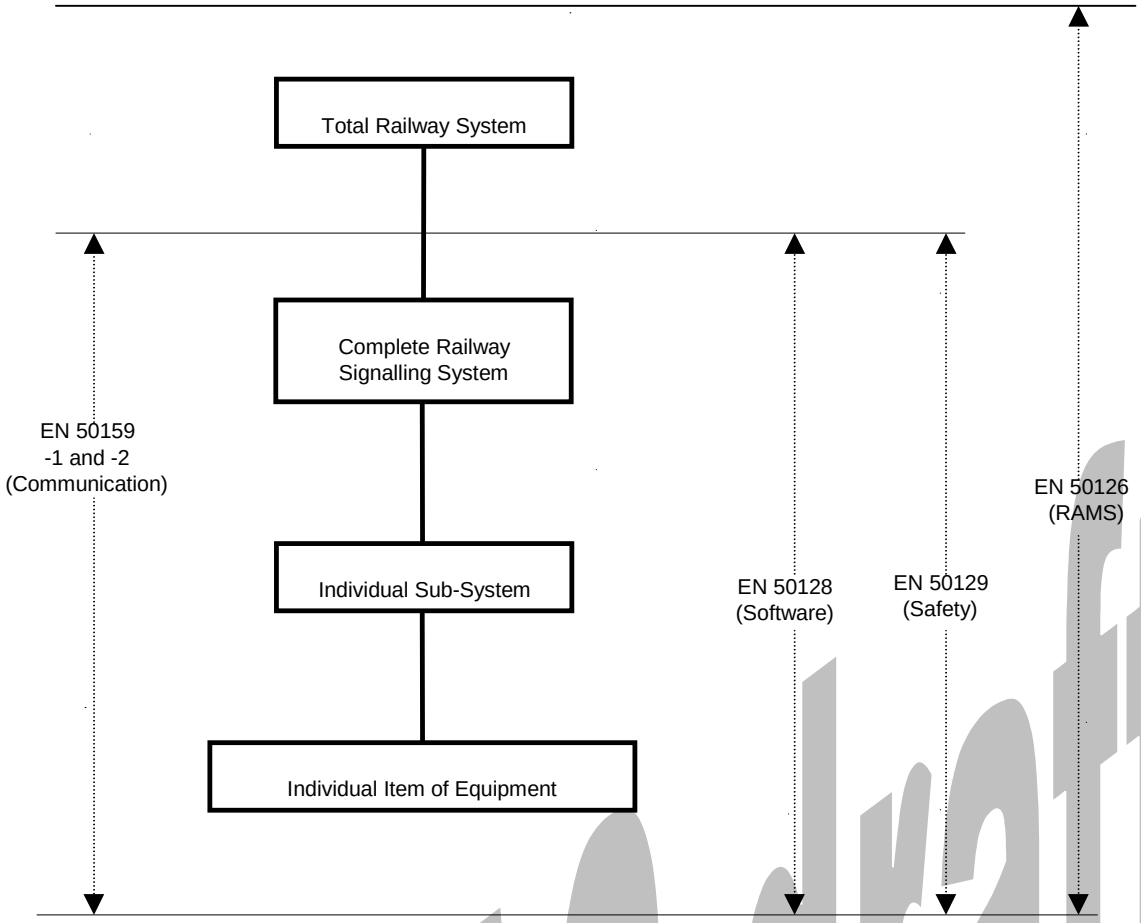


Figure 1: Scope of the main CENELEC railway application standards

2 Normative references

This European Standard incorporates, by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

NOTE: Additional informative references are included in annex F: Bibliography.

EN 50121-2	Railway Applications: Electromagnetic compatibility (EMC) - Interaction of the whole railway system with the outside world.
EN 50121-3	Railway Applications: Electromagnetic compatibility (EMC) - Rolling stock.
EN 50121-4	Railway Applications: Electromagnetic compatibility (EMC) - Signalling and communications.
EN 50124-1	Railway Applications: Insulation co-ordination – Part 1: Basic requirements; clearances and creepage distances.
EN 50124-2	Railway Applications: Insulation co-ordination – Part 2: Overvoltages and related protection
EN 50125-1	Railway Applications: Environmental conditions for equipment - Equipment on board rolling stock.
EN 50125-3	Railway Applications: Environmental conditions for equipment - Signalling and communications.
EN 50126	Railway Applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
EN 50128	Railway Applications: Software for railway control and protection systems.
EN 50155	Railway Applications: Electronic equipment used on rail vehicles.
EN 50159-1	Railway Applications: Signalling and communications - Safety-related communication in closed transmission systems.
EN 50159-2	Railway Applications: Signalling and communications - Safety-related communication in open transmission systems.

3 Definitions and Abbreviations

3.1 Definitions

For the purposes of this standard, the following definitions apply:

3.1.1 accident

An unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage.

3.1.2 assessment

The process of analysis to determine whether the design authority and the validator have achieved a product that meets the specified requirements and to form a judgement as to whether the product is fit for its intended purpose.

3.1.3 authorisation

The formal permission to use a product within specified application constraints.

3.1.4 availability

The ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided.

3.1.5 can

Is possible.

3.1.6 causal analysis

Analysis of the reasons how and why a particular hazard may come into existence.

3.1.7 common-cause failure

Failure common to items which are intended to be independent.

3.1.8 consequence analysis

Analysis of events which are likely to happen after a hazard has occurred.

3.1.9 configuration

The structuring and interconnection of the hardware and software of a system for its intended application.

3.1.10 cross-acceptance

The status achieved by a product that has been accepted by one authority to the relevant European Standards and is acceptable to other authorities without the necessity for further assessment.

3.1.11 design

The activity applied in order to analyse and transform specified requirements into acceptable design solutions which have the required safety integrity.

3.1.12 design authority

The body responsible for the formulation of a design solution to fulfil the specified requirements and for overseeing the subsequent development and setting-to-work of a system in its intended environment.

3.1.13 diversity

A means of achieving all or part of the specified requirements in more than one independent and dissimilar manner.

3.1.14 equipment

A functional physical item.

3.1.15 error

A deviation from the intended design which could result in unintended system behaviour or failure.

3.1.16 fail-safe

A concept which is incorporated into the design of a product such that, in the event of a failure, it enters or remains in a safe state.

3.1.17 failure

A deviation from the specified performance of a system. A failure is the consequence of an fault or error in the system.

3.1.18 fault

An abnormal condition that could lead to an error in a system. A fault can be random or systematic.

3.1.19 fault detection time

Time span which begins at the instant when a fault occurs and ends when the existence of the fault is detected.

3.1.20 function

A mode of action or activity by which a product fulfils its purpose.

3.1.21 hazard

A condition that could lead to an accident.

3.1.22 hazard analysis

The process of analysing the causes of hazards and of identification of requirements to limit the likelihood of hazards to a tolerable level.

3.1.23 hazard log

The document in which all safety management activities, hazards identified, decisions made and solutions adopted, are recorded or referenced.

3.1.24 human error

A human action (mistake), which can result in unintended system behaviour/failure.

3.1.25 implementation

The activity applied in order to transform the specified designs into their physical realisation.

3.1.26 independence (functional)

Freedom from any mechanism which can affect the correct operation of more than one function as a result of either systematic or random failure.

3.1.27 independence (human)

Freedom from intellectual, commercial and/or management involvement.

3.1.28 independence (physical)

Freedom from any mechanism which can affect the correct operation of more than one system/sub-system/equipment as a result of random failures.

3.1.29 individual risk

A risk which is related to a single individual only.

3.1.30 maintainability

The probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources.

3.1.31 maintenance

The combination of all technical and administrative actions, including supervision actions, intended to retain an item in, or restore it to, a state in which it can perform its required function.

3.1.32 may

Is permissible.

3.1.33 negation

Enforcement of a safe state following detection of a hazardous fault.

3.1.34 negation time

Time span which begins when the existence of a fault is detected and ends when a safe state is enforced.

3.1.35 product

A collection of elements, interconnected to form a system/sub-system/equipment, in a manner which meets the specified requirements.

3.1.36 quality

A user perception of the attributes of a product.

3.1.37 railway authority

The body with the overall accountability to a safety authority for operating a safe railway system.

3.1.38 random failure integrity

The degree to which a system is free from hazardous random faults.

3.1.39 random fault

The occurrence of a fault based on probability theory and previous performance.

3.1.40 redundancy

The provision of one or more additional elements, usually identical, to achieve or maintain availability under the failure of one or more of those elements.

3.1.41 reliability

The ability of an item to perform a required function under given conditions for a given period of time.

3.1.42 repair

Measures for re-establishing the required state of a system/sub-system/equipment.

3.1.43 risk

The combination of the frequency, or probability, and the consequence of a specified hazardous event.

3.1.44 safe state

A condition which continues to preserve safety.

3.1.45 safety

Freedom from unacceptable levels of risk.

3.1.46 safety acceptance

The safety status given to a product by the final user.

3.1.47 safety approval

The safety status given to a product by the requisite authority when the product has fulfilled a set of pre-determined conditions.

3.1.48 safety authority

The body responsible for certifying that a safety-related system is fit for service and complies with relevant statutory and regulatory safety requirements.

3.1.49 safety case

The documented demonstration that the product complies with the specified safety requirements.

3.1.50 safety integrity

The likelihood of a safety-related system achieving its required safety features under all the stated conditions within a stated operational environment and within a stated period of time.

3.1.51 safety integrity level

Freedom from any mechanism which can affect the correct operation of more than one system/sub-system/equipment as a result of random failures.

3.1.52 safety life-cycle

The additional series of activities carried out in conjunction with the system life-cycle for safety-related systems.

3.1.53 safety management

The management structure which ensures that the safety process is properly implemented.

3.1.54 safety plan

The implementation details of how the safety requirements of the project will be achieved.

3.1.55 safety process

The series of procedures that are followed to enable all safety requirements of a product to be identified and met.

3.1.56 safety-related

Carries responsibility for safety.

3.1.57 shall

Is mandatory.

3.1.58 should

Is recommended.

3.1.59 signalling system

Particular kind of system used on a railway to control and protect the operation of trains.

3.1.60 stress profile

The degree and number of external influences which a product can withstand whilst performing its required functionality.

3.1.61 sub-system

A portion of a system which fulfils a specialised function.

3.1.62 system

A set of sub-systems which interact according to a design.

3.1.63 systematic failure integrity

The degree to which a system is free from non-identified hazardous errors and the causes thereof.

3.1.64 systematic fault

An inherent fault in the specification, design, construction, installation, operation or maintenance of a system, sub-system or equipment.

3.1.65 system life-cycle

The series of activities occurring during a period of time that starts when a system is conceived and ends at decommissioning when the system is no longer available for use.

3.1.66 technical safety report

Documented technical evidence for the safety of the design of a system/sub-system/equipment.

3.1.67 validation

The activity applied in order to demonstrate, by test and analysis, that the product meets in all respects its specified requirements.

3.1.68 verification

The activity of determination, by analysis and test, *at* each phase of the life-cycle, that the requirements of the phase meet the output of the previous phase and that the output of the phase fulfils its requirements.

3.2 Abbreviations

For the purposes of this standard, the following abbreviations apply:

3.2.1	**AC**	Alternating Current
3.2.2	**ATP**	Automatic Train Protection
3.2.3	**CENELEC**	European Committee for Electrotechnical Standardisation
3.2.4	**CCF**	Common-Cause Failure
3.2.5	**DC**	Direct Current
3.2.6	**EMC**	Electromagnetic Compatibility
3.2.7	**EMI**	Electromagnetic Interference
3.2.8	**EN**	European Norm
3.2.9	**ESD**	Electrostatic Discharge
3.2.10	**FET**	Field Effect Transistor
3.2.11	**FMEA**	Failure Modes and Effects Analysis
3.2.12	**FTA**	Fault Tree Analysis
3.2.13	**HW**	Hardware
3.2.14	**IEC**	International Electrotechnical Commission
3.2.15	**IRSE**	Institution of Railway Signal Engineers
3.2.16	**ISO**	International Standards Organisation
3.2.17	**RAMS**	Reliability, Availability, Maintainability and Safety
3.2.18	**SCR**	Silicon Controlled Rectifier
3.2.19	**SIL**	Safety Integrity Level
3.2.20	**SW**	Software
3.2.21	**THR**	Tolerable hazard rate
3.2.22	**UIC**	International Union of Railways
3.2.23	**VDR**	Voltage-Dependent Resistor

4 Overall framework of this standard

Section 5 of this European Standard EN 50129 requires that a systematic, documented approach be taken to:

- Evidence of quality management
- Evidence of safety management
- Evidence of functional and technical safety
- Safety acceptance and approval.

Annex A (Normative) defines the interpretation and use of Safety Integrity Levels.

Annex B (Normative) contains detailed technical requirements for safety-related systems/sub-systems/equipment.

Annex C (Normative) contains procedures and information for identifying the credible failure modes of hardware components.

Annex D (Informative) contains supplementary technical information.

Annex E (Informative) contains tables of techniques/measures to be used for various levels of safety integrity.

Annex F (Informative) contains references to documents that have been consulted during the preparation of this standard.

The structure of this standard is summarised in figure 2.

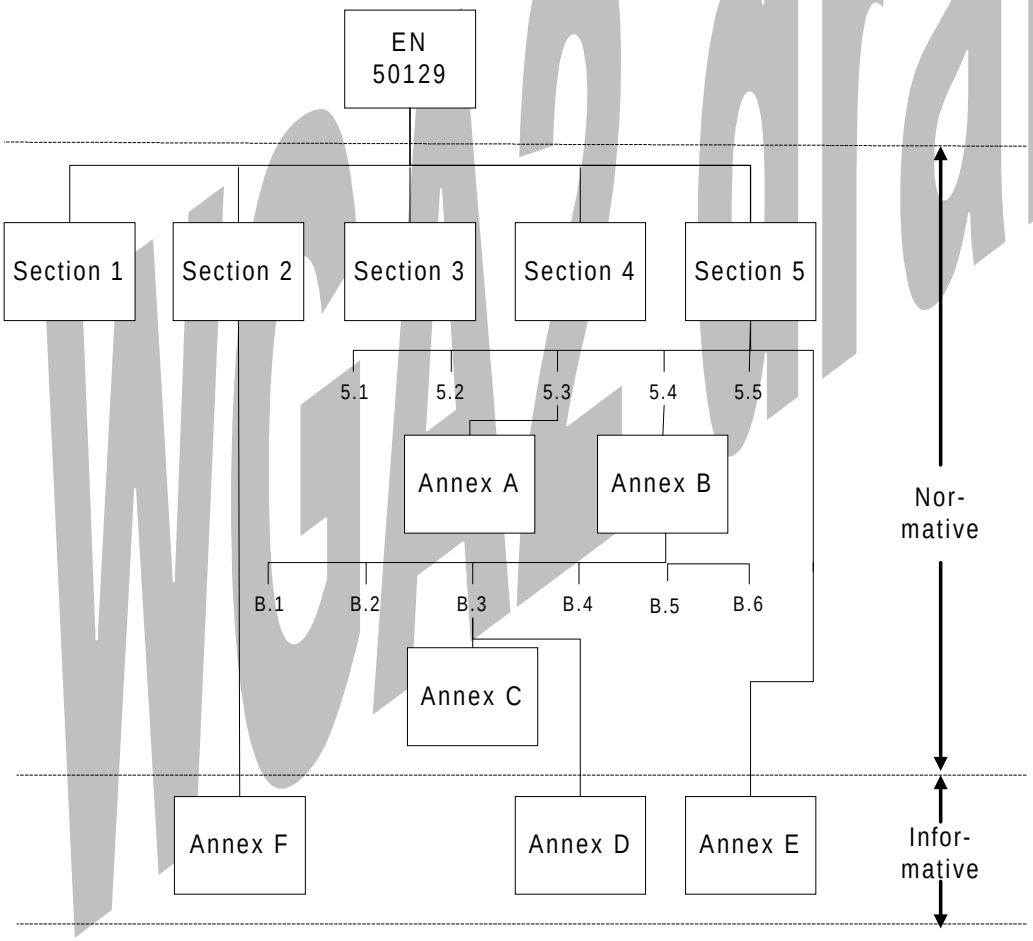


Figure 2: Structure of this standard (EN 50129)

5 Conditions for safety acceptance and approval

5.1 The Safety Case

This standard defines the conditions that shall be satisfied in order that a safety-related electronic railway system/sub-system/equipment can be accepted as adequately safe for its intended application.

The conditions for safety acceptance are presented in this standard under three headings, namely:

5.2 Evidence of quality management;
5.3 Evidence of safety management;
5.4 Evidence of functional and technical safety.

All of these conditions shall be satisfied, at equipment, sub-system and system levels, before the safety-related system can be accepted as adequately safe.

The documentary evidence that these conditions have been satisfied shall be included in a structured safety justification document, known as the Safety Case. The Safety Case forms part of the overall documentary evidence to be submitted to the relevant safety authority in order to obtain safety approval for a generic product, a class of application or a specific application. For an explanation of the safety approval process, see sub-clause 5.5 of this standard.

The Safety Case contains the documented safety evidence for the system/sub-system/equipment, and shall be structured as follows:

Part 1. Definition of System (or sub-system/equipment)

This shall precisely define or reference the system/sub-system/equipment to which the Safety Case refers, including version numbers and modification status of all requirements, design and application documentation.

Part 2. Quality Management Report

This shall contain the evidence of quality management, as specified in sub-clause 5.2 of this standard.

Part 3. Safety Management Report

This shall contain the evidence of safety management, as specified in sub-clause 5.3 of this standard.

Part 4. Technical Safety Report

This shall contain the evidence of functional and technical Safety, as specified in sub-clause 5.4 of this standard.

Part 5. Related Safety Cases

This shall contain references to the Safety Cases of any sub-systems or equipment on which the main Safety Case depends.

This section shall also demonstrate that all the safety-related application conditions specified in each of the related sub-system/equipment Safety Cases are,

either: fulfilled in the main Safety Case;

or: carried forward into the safety-related application conditions of the main Safety Case.

Part 6. Conclusion

This shall summarise the evidence presented in the previous parts of the Safety Case, and argue that the relevant system/sub-system/equipment is adequately safe, subject to compliance with the specified application conditions.

The structure of the Safety Case is illustrated in figure 3 of this standard.

Large volumes of detailed evidence and supporting documentation need not be included in the Safety Case and in its parts, provided precise references are given to such documents and provided the base concepts used and the approaches taken are clearly specified.

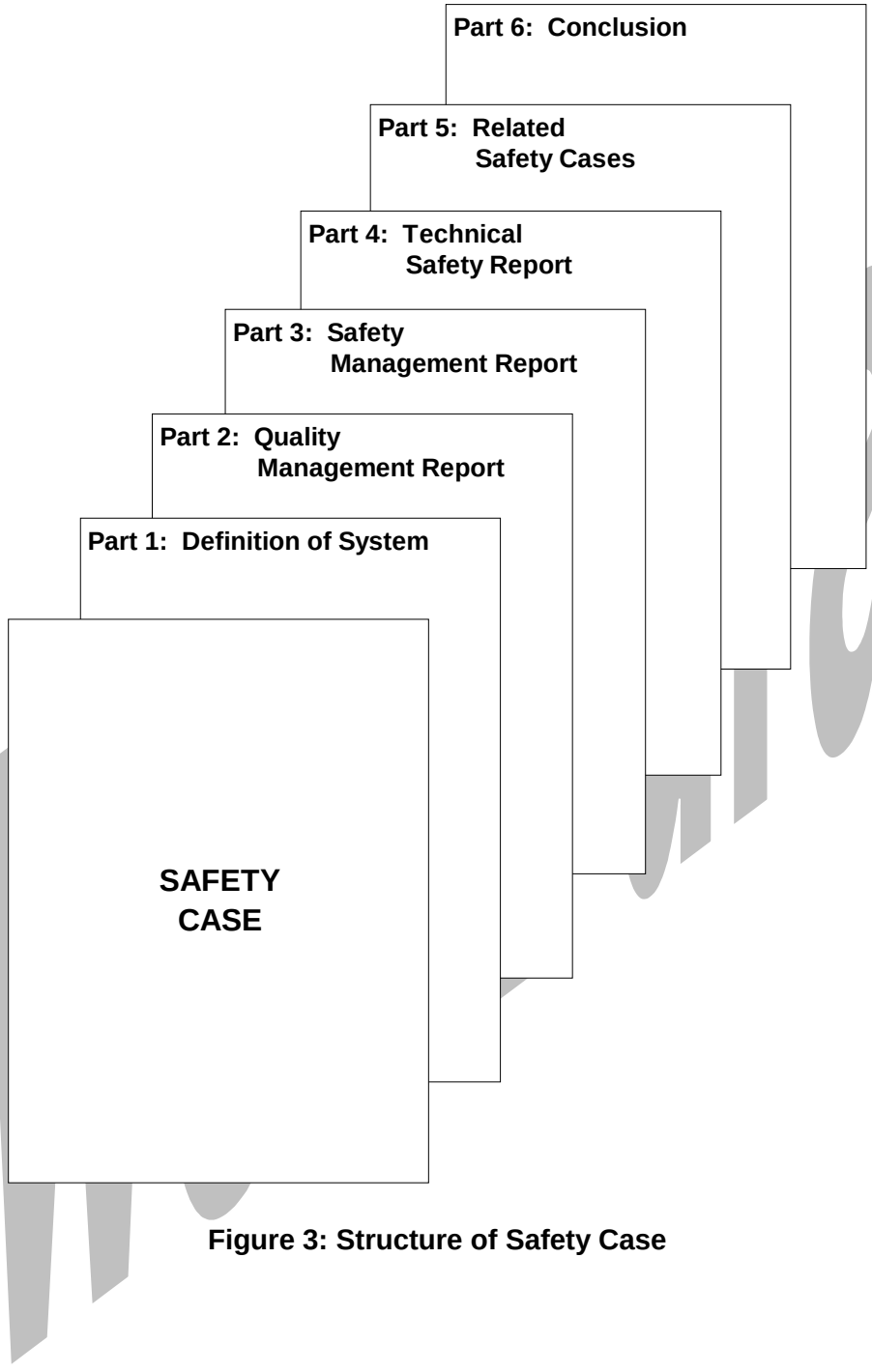


Figure 3: Structure of Safety Case

5.2 Evidence of quality management

The first condition for safety acceptance that shall be satisfied is that the quality of the system, sub-system or equipment has been, and shall continue to be, controlled by an effective quality management system throughout its life-cycle. Documentary evidence to demonstrate this shall be provided in the Quality Management Report, which forms part 2 of the Safety Case.

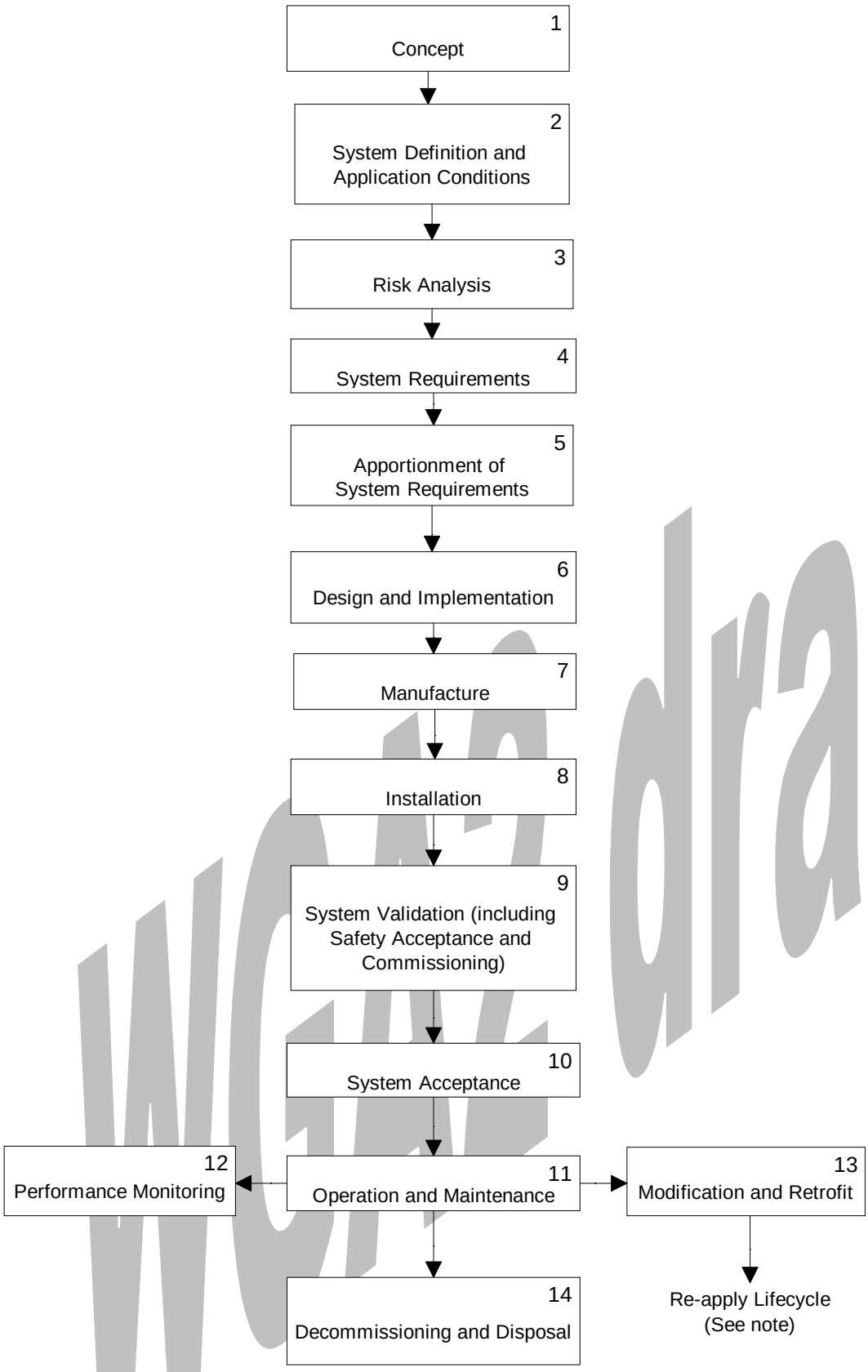
The purpose of the quality management system is to minimise the incidence of human errors at each stage in the life-cycle, and thus to reduce the risk of systematic faults in the system, sub-system or equipment.

The quality management system shall be applicable throughout the system/sub-system/equipment life-cycle, as defined in EN 50126. An example of a system life-cycle diagram (from EN 50126) is reproduced as figure 4 of this standard.

NOTE: Examples of aspects (based on ISO 9001) which should be controlled by the quality management system and included in the Quality Management Report:

- Organisational structure;
- Quality planning and procedures;
- Specification of requirements;
- Design control;
- Design verification and reviews;
- Application engineering;
- Procurement and manufacture;
- Product identification and traceability;
- Handling and storage;
- Inspection and testing;
- Non-conformance and corrective action;
- Packaging and delivery;
- Installation and commissioning;
- Operation and maintenance;
- Quality monitoring and feedback;
- Documentation and records;
- Configuration management/change control;
- Personnel competency and training;
- Quality audits and follow-up;
- Decommissioning and disposal.

Compliance with the requirements for quality management is mandatory for Safety Integrity Levels 1 to 4 inclusive, (see annex A for explanation of Safety Integrity Levels). However, the depth of the evidence presented and the extent of the supporting documentation should be appropriate to the Safety Integrity Level of the system/sub-system/equipment under scrutiny (see annex E, tables E.1 and E.8 for guidance on evidence required for each Safety Integrity Level). The requirements for Safety Integrity Level 0 (non-safety-related) are outside the scope of this safety standard.



Note: The phase at which a modification enters the life-cycle will be dependent upon both the system being modified and the specific modification under consideration.

Figure 4: Example of system life-cycle (from EN 50126)

5.3 Evidence of safety management

5.3.1 Introduction

The second condition for safety acceptance which shall be satisfied is that the safety of the system, sub-system or equipment has been, and shall continue to be, managed by means of an effective safety management process, which should be consistent with the management process for RAMS described in EN 50126. The purpose of this process is to further reduce the incidence of safety-related human errors throughout the life-cycle, and thus minimise the residual risk of safety-related systematic faults. The elements of the safety management process are briefly summarised in paragraphs 5.3.2 to 5.3.13 below.

Documentary evidence to demonstrate compliance with all elements of the safety management process throughout the life-cycle shall be provided in the Safety Management Report, which forms Part 3 of the Safety Case. Large volumes of detailed evidence and supporting documentation need not be included, provided precise references are given to such documents.

The use of this safety management process is mandatory for Safety Integrity Levels 1 to 4 inclusive (see annex A for explanation of Safety Integrity Levels). However, the depth of the evidence presented and the extent of the supporting documentation should be appropriate to the Safety Integrity Level of the system/sub-system/equipment under scrutiny. The requirements for Safety Integrity Level 0 (non-safety-related) are outside the scope of this safety standard.

> NOTE: In all cases the hazard analysis and risk assessment processes defined in EN 50126 are necessary, in order to identify the required level of safety integrity for each particular situation. This includes those cases where the analysis and assessment reveal that a Safety Integrity Level of zero may be assigned; however, once this conclusion has been reached (i.e. that the situation is non-safety-related), and provided it remains at level zero, this safety standard ceases to be applicable.

5.3.2 Safety life-cycle

The safety management process shall consist of a number of phases and activities, which are linked to form the safety life-cycle; this should be consistent with the system life-cycle defined in EN 50126, which is reproduced as figure 4 of this standard. The design and validation part of the system life-cycle can be viewed as a "top-down" phase followed by a "bottom-up" phase, (i.e. a "V" - diagram), an example of which is shown in figure 5 of this standard.

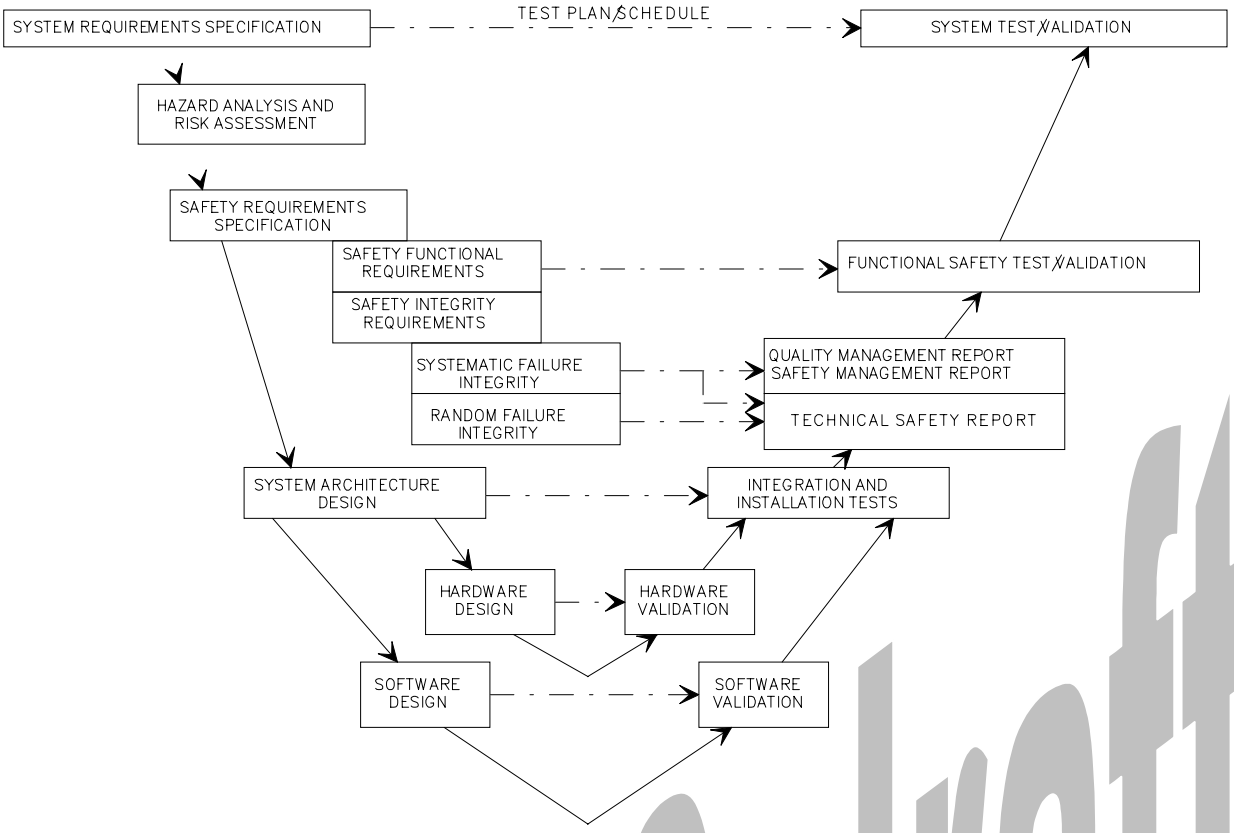


Figure 5: Example of design and validation portion of system life-cycle

5.3.3 Safety organisation

The safety management process shall be implemented under the control of an appropriate safety organisation, using competent personnel assigned to specific roles. Assessment and documentation of personnel competence, including technical knowledge, qualifications, relevant experience and appropriate training, shall be carried out in accordance with recognised standards. An appropriate degree of independence shall be provided between different roles, as shown in figure 6 of this standard. See also annex E, table E.3, for guidance on the safety organisation required for each Safety Integrity Level.

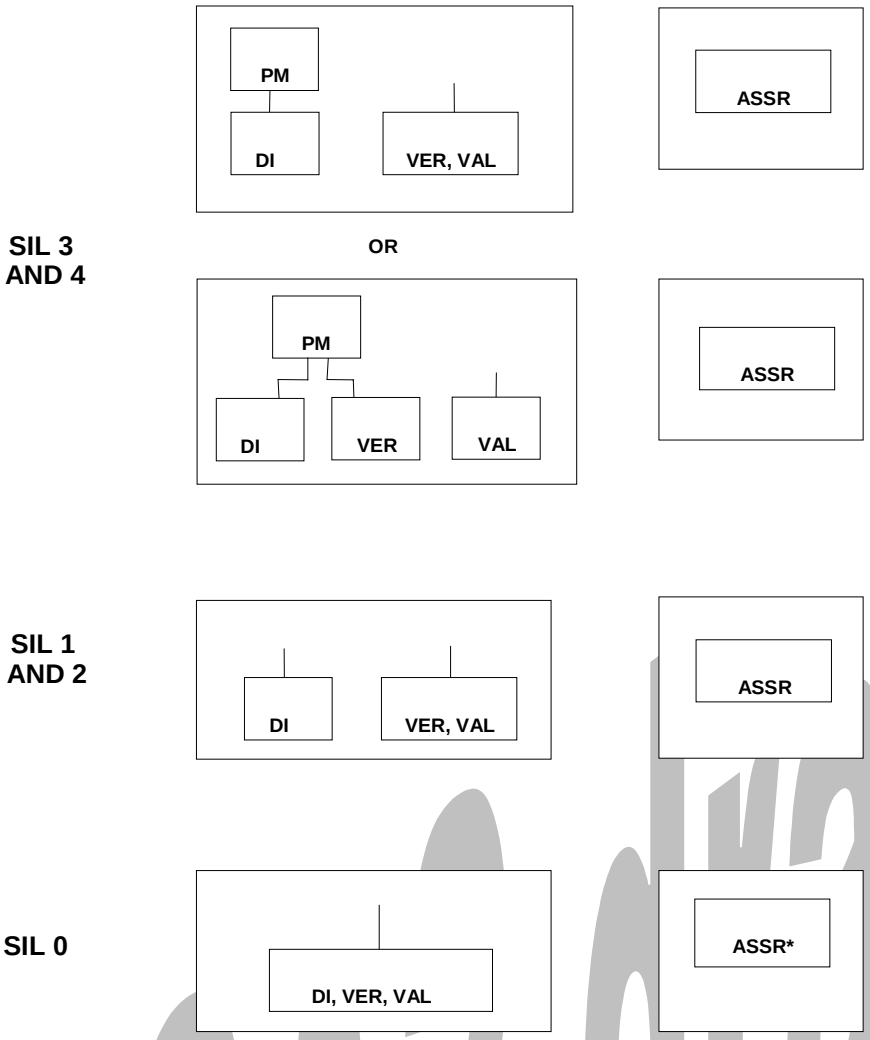


Figure 6: Arrangements for independence

5.3.4 Safety plan

A Safety Plan shall be drawn up at the start of the life-cycle. This plan shall identify the safety management structure, safety-related activities and approval mile-stones throughout the life-cycle, and shall include the requirements for review of the Safety Plan at appropriate intervals. The Safety Plan shall be updated and reviewed if subsequent alterations or additions are made to the original system/sub-system/equipment. If any such change is made, the effect on safety shall be assessed, starting at the appropriate point in the life-cycle. See annex E, table E.1, for guidance on Safety Plans for each Safety Integrity Level.

The Safety Plan shall deal with all aspects of the system/sub-system/equipment, including both hardware and software. EN 50128 shall be referenced for Software aspects.

The Safety Plan should include a Safety Case Plan, which identifies the intended structure and principal components of the final Safety Case.

5.3.5 Hazard log

A Hazard Log shall be created and maintained throughout the safety life-cycle, as explained in EN 50126. It shall include a list of identified hazards, together with associated risk classification and risk control information for each hazard. The Hazard Log shall be updated if any modification or alteration is made to the system, sub-system or equipment.

5.3.6 Safety requirements specification

The specific safety requirements for each system/sub-system/equipment, including safety functions and safety integrity, shall be identified and documented in the Safety Requirements Specification. This shall be achieved by means of:

- Hazard Identification and Analysis;
- Risk Assessment and Classification;
- allocation of Safety Integrity Levels,

as explained in EN 50126. Some information concerning Safety Integrity Levels for railway electronic systems is contained in annex A.

NOTE: The Safety Requirements Specification may be included in the system/sub-system/equipment Functional Requirements Specification or may be written as a separate document. See annex E, table E.2, for guidance on System Requirements Specifications for each Safety Integrity Level.

5.3.7 System/sub-system/equipment design

This phase of the life-cycle shall create a design which fulfils the specified operational and safety requirements. A top-down, structured design methodology shall be used, with rigorously controlled and reviewed documentation. In particular, the relationship between hardware and software, as represented by the Software Requirements Specification and software/hardware integration, shall be strictly managed, and the standard EN 50128 shall be adhered to. Annex E, table E.7, gives guidance on design and development of system/sub-system/equipment for each Safety Integrity Level.

5.3.8 Safety reviews

Safety reviews shall be carried out at appropriate stages in the life-cycle. Such reviews shall be specified in the Safety Plan, and their results fully documented. Any alteration or extension to the system, sub-system or equipment shall also be subject to review.

5.3.9 Safety verification and validation

The Safety Plan shall include or reference plans for verifying that each phase of the life-cycle satisfies the specific safety requirements identified in the previous phase, and for validating the completed system/sub-system/equipment against its original Safety Requirements Specification.

These activities shall be carried out and fully documented, including appropriate testing and safety analyses. They shall be repeated as appropriate in the event of any subsequent modification or addition to the system/sub-system/equipment.

The degree of independence necessary for the verifier and the validator shall be in accordance with the Safety Integrity Level of the system/sub-system/equipment under scrutiny. This is shown in figure 6. Annex E, table E.9, gives guidance on verification and validation techniques/measures for each Safety Integrity Level.

At the discretion of the safety authority, the assessor may be part of the supplier's organisation or of the customer's organisation but, in such cases, the assessor shall:

- be authorised by the safety authority
- be totally independent from the project team
- report directly to the safety authority.

5.3.10 Safety justification

The evidence that the system/sub-system/equipment meets the defined conditions for safety acceptance shall be presented in a structured safety justification document known as the Safety Case, as explained in sub-clause 5.1 of this standard.

5.3.11 System/sub-system/equipment handover

Prior to handover of the system/sub-system/equipment to a railway authority, the conditions for safety acceptance and safety approval defined in sub-clause 5.5 shall be satisfied, including submission of the Safety Case and the Safety Assessment Report.

5.3.12 Operation and maintenance

Following handover, the procedures, support systems and safety monitoring defined in the Safety Plan and in chapter 5 of the Technical Safety Report (part of the Safety Case) shall be adhered to.

During the operational life of a system, change requests may be raised for a variety of reasons, not all of which will be safety-related. Each change request shall be assessed for its impact on safety, by reference to the relevant portion of the safety documentation. Where a change request results in a modification which could affect the safety of the system, or associated systems, or the environment, the appropriate portion of the safety life-cycle shall be repeated to ensure that the implemented modification does not unacceptably reduce the level of safety. Annex E, table E.10, gives guidance Application, Operation and Maintenance for each Safety Integrity Level.

5.3.13 Decommissioning and disposal

At the end of the operational life of a system, its decommissioning and disposal shall be carried out in accordance with the measures defined in the Safety Plan and in chapter 5 of the Technical Safety Report (part of the Safety Case).

5.4 Evidence of functional and technical safety

In addition to the evidence of quality and safety management, described in subsections 5.2 and 5.3 of this standard, a third condition shall be satisfied before a system/sub-system/equipment can be accepted as adequately safe for its intended application. This consists of technical evidence for the safety of the design, which shall be documented in the Technical Safety Report. This document forms Part 4 of the Safety Case for the system/sub-system/equipment, as explained in sub-clause 5.1 of this standard.

The Technical Safety Report is mandatory for Safety Integrity Levels 1 to 4 inclusive (see annex A for explanation of Safety Integrity Levels). However, the depth of the information and the extent of the supporting documentation should be appropriate to the Safety Integrity Level of the system/sub-system/equipment under scrutiny. The requirements for Safety Integrity Level 0 (non-safety-related) are outside the scope of this safety standard.

The Technical Safety Report shall explain the technical principles which assure the safety of the design, including (or giving references to) all supporting evidence (for example, design principles and calculations, test specifications and results, and safety analyses).

The Technical Safety Report shall be arranged under the following headings:

Section 1. Introduction

This section shall provide an overview description of the design, including a summary of the technical safety principles that are relied on for safety and the extent to which the system/sub-system/equipment is claimed to be safe in accordance with this standard.

This section shall also indicate the standards (and their issues) used as the basis for the technical safety of the design. In the case of modifications or additions to equipment already in service, or in standard production, or at a completed stage of development, then, as an exception, the issues of standards used for the original design may be used as a basis, these already having been accepted in the approval of the original equipment. This may be applied only if, by taking into consideration the latest issues of the standards, further modifications to the existing equipment would be required, or unjustifiably high costs for the change would be incurred. Reasons justifying use of this statement shall be given.

Section 2. Assurance of correct functional operation

This section shall contain all the evidence necessary to demonstrate correct operation of the system/sub-system/equipment under fault-free normal conditions (that is, with no faults in existence), in accordance with the specified operational and safety requirements.

The following aspects shall be included, for which more detailed requirements are contained in annex B.2:

2.1 System architecture description (see annex B.2.1 and annex E, table E.4);
2.2 Definition of interfaces (see annex B.2.2);
2.3 Fulfilment of System Requirements Specification (see annex B.2.3);
2.4 Fulfilment of Safety Requirements Specification (see annex B.2.4);
2.5 Assurance of correct hardware functionality (see annex B.2.5);
2.6 Assurance of correct software functionality (see annex B.2.6).

Section 3. Effects of faults

This section shall demonstrate that the system/sub-system/equipment continues to meet its specified safety requirements, including the quantified safety target, in the event of random hardware faults.

In addition, a systematic fault could still exist, despite the quality and safety management processes defined in sub-clauses 5.2 and 5.3 of this standard. This section shall demonstrate which technical measures have been taken to reduce the consequent risk to a level that is as low as reasonably practicable.

This section shall also include demonstration that faults in any system/sub-system/equipment having a Safety Integrity Level lower than that of the overall system, including Level 0, cannot reduce the safety of the overall system.

The following headings shall be used in this section, for which more detailed requirements are contained in annex B.3. Guidance is also given in annex E, tables E.5 and E6.

3.1 Results of single faults (see annex B.3.1);
3.2 Independence of items (see annex B.3.2);
3.3 Detection of single faults (see annex B.3.3);
3.4 Action following detection (including retention of safe state) (see annex B.3.4);
3.5 Effects of multiple faults (see annex B.3.5);
3.6 Defence against systematic faults (see annex B.3.6).

Section 4. Operation with external influences

This section shall demonstrate that when subjected to the external influences defined in the System Requirements Specification, the system/sub-system/equipment:

- Continues to fulfil its specified operational requirements;
- Continues to fulfil its specified safety requirements (including fault conditions).

The Safety Case is therefore valid only within the specified range of external influences, as defined in the System Requirements Specification. Safety is not assured outside these limits, unless additional special measures are provided.

The methods used to withstand the specified external influences shall be fully explained and justified.

More detailed requirements are contained in annex B.4.

Section 5. Safety-related application conditions

This section shall specify (or reference) the rules, conditions and constraints which shall be observed in the application of the system/sub-system/equipment. This shall include the application conditions contained in the Safety Case of any related sub-system or equipment.

More detailed requirements are contained in annex B.5. Guidance is also given in annex E, table E.10.

Section 6. Safety Qualification Tests

This section shall contain evidence to demonstrate successful completion, under operational conditions, of the Safety Qualification Tests. These are explained in annex B.6.

The structure of the Technical Safety Report is illustrated in figure 7 of this standard.

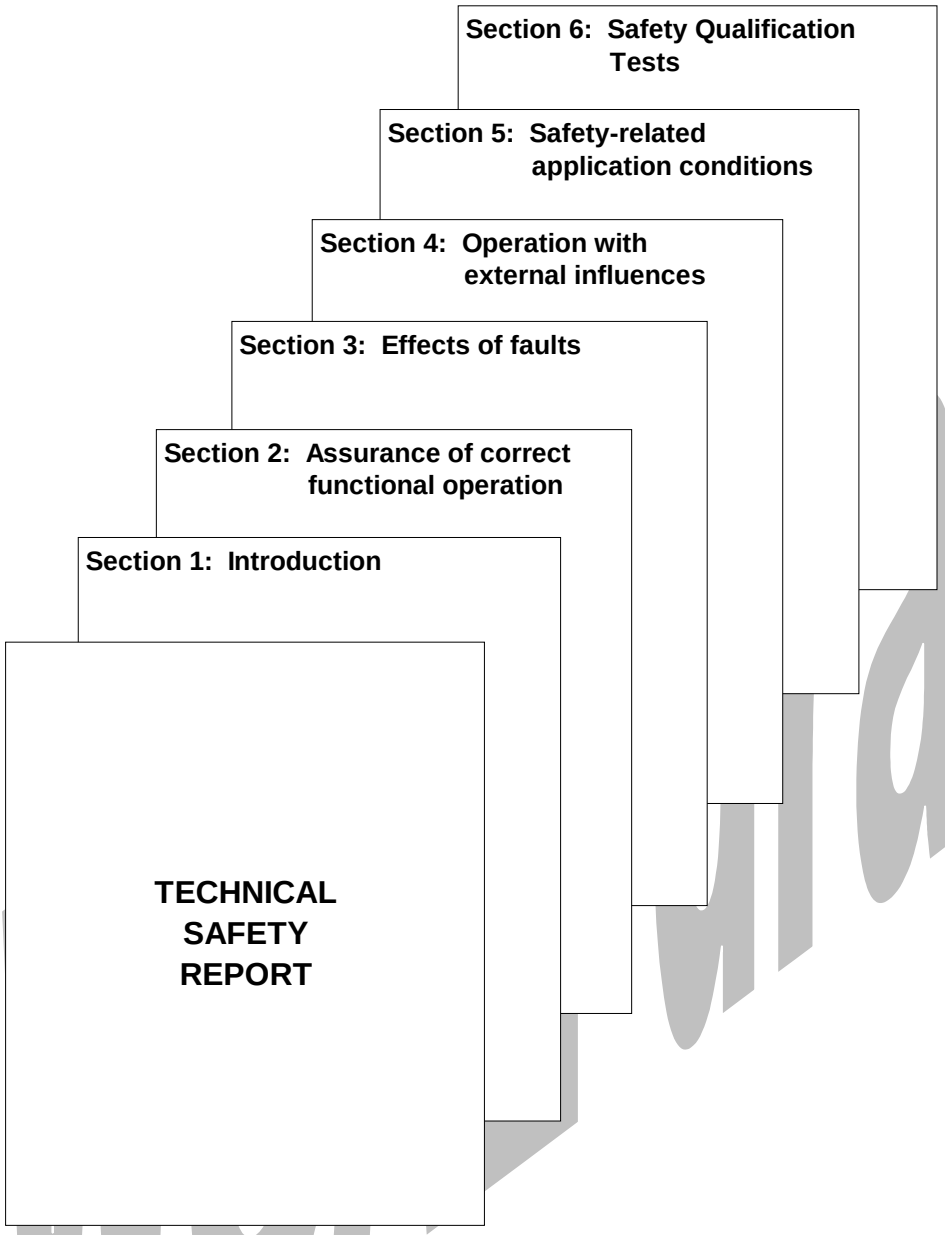


Figure 7: Structure of Technical Safety Report

5.5 Safety acceptance and approval

This sub-clause defines the safety acceptance and approval process for safety-related electronic system/sub-system/equipment. Except where considered appropriate, it does not specify who should carry out the work at each stage, since this may vary in different circumstances.

5.5.1 Introduction

As explained in sub-clause 5.1 of this standard, three conditions shall be satisfied before a safety-related electronic railway system/sub-system/equipment can be accepted as adequately safe for its intended application:

- **Evidence of quality management;**
- **Evidence of safety management;**
- **Evidence of functional and technical safety.**

These three conditions have been explained in sub-clauses 5.2, 5.3 and 5.4 of this standard.

The evidence of quality management, safety management and functional/technical safety shall be included in the Safety Case, as shown in sub-clause 5.1 and figure 3.

Three different categories of Safety Case can be considered:

- **Generic product Safety Case** (independent of application)
  A generic product can be re-used for different independent applications.
- **Generic application Safety Case** (for a class of application)
  A generic application can be re-used for a class/type of application with common functions.
- **Specific application Safety Case** (for a specific application)
  A specific application is used for only one particular installation.

It is essential to demonstrate for each ”specific” application that the environmental conditions and context of use are compatible with the ”generic” application conditions (paragraph 5.5.4).

In all three categories, the structure of the Safety Case and the procedure for obtaining Safety approval are basically the same. However, there is an additional factor for specific applications : in this category, separate Safety approval is needed for the application design of the system and for its physical implementation (e.g., manufacture, installation, test, and facilities for operation and maintenance). For this reason, the Safety Case for specific applications shall be divided into two portions:

- The Application Design Safety Case: this shall contain the safety evidence for the theoretical design of the specific application.
- The physical implementation Safety Case: this shall contain the safety evidence for the physical implementation of the specific application.

Both portions shall be structured as shown in sub-clause 5.1 and figure 3 of this standard.

5.5.2 Safety approval process

Before an application for Safety approval can be considered, an independent safety assessment of the system/sub-system/equipment and its Safety Case shall be carried out, to provide additional assurance that the necessary level of safety has been achieved. Its results should be presented in a Safety Assessment Report. The report should explain the activities carried out by the safety assessor to determine how the system/sub-system/equipment, (hardware and software) has been designed to meet its specified requirements, and possibly specify some additional conditions for the operation of the system/sub-system/equipment. The depth of the safety assessment, and the degree of independence with which it is carried out, are based on the results of the risk classification, as explained in EN 50126. Specific tests may be required by the safety assessor in order to increase confidence.

The overall documentary evidence shall consist of:

- **The System (or sub-system/equipment) Requirements Specification;**
- **The Safety Requirements Specification;**
- **The Safety Case, including:**

  Part 1: Definition of System/Sub-system/Equipment;
  Part 2: Quality Management Report (evidence of Quality Management);
  Part 3: Safety Management Report (evidence of Safety Management);
  Part 4: Technical Safety Report (evidence of Functional/Technical Safety);
  Part 5: Related Safety Cases (if applicable);
  Part 6: Conclusion;

- **The Safety Assessment Report.**

Provided all the conditions for safety acceptance have been satisfied, as demonstrated by the Safety Case, and subject to the results of the independent safety assessment, the system/sub-system/equipment may be granted safety approval by the relevant safety authority. Approval may be subject to the fulfilment of additional conditions (temporary or permanent) imposed by the safety assessor.

For a generic product (i.e.: independent of application), and for a generic application (i.e.: class of application), it should be possible for safety approval granted by one safety authority to be accepted by other safety authorities (i.e.: cross-acceptance). This is not considered possible for specific applications**.**

The safety approval process, for all three categories of Safety Case, is illustrated in figure 8.

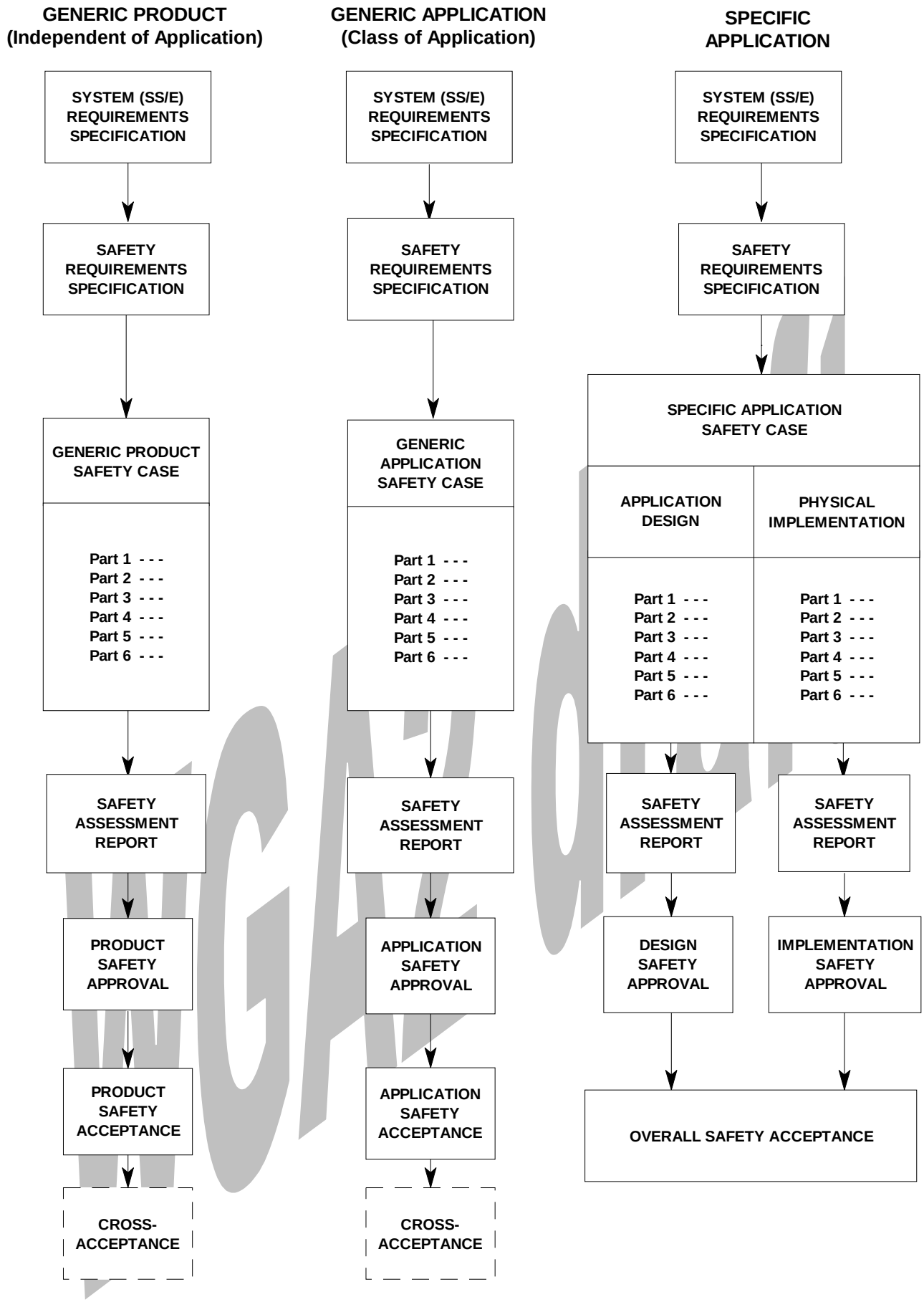


Figure 8: Safety acceptance and approval process

5.5.3 After safety approval

After a system/sub-system/equipment has received safety approval, any subsequent modification shall be controlled using the same quality management, safety management and functional/technical safety criteria as would be used for a new design. All relevant documentation, including the Safety Case, shall be updated or supplemented by additional documentation, and the modified design shall be submitted for approval.

Once an installed system/sub-system/equipment has been commissioned, appropriate procedures, support systems and safety monitoring, as defined in the Safety Plan and in chapter 5 of the Technical Safety Report (part of the Safety Case), shall be used to ensure continued safe operation throughout its working life, including operation, maintenance, alteration, extension and eventual decommissioning. These activities shall be controlled using the same quality management, safety management and technical safety criteria as for the original design. All relevant documentation shall be kept up-to-date, including the Safety Case, and any alterations or extensions shall be submitted for approval.

5.5.4 Dependency between safety approvals

As mentioned in sub-clause 5.1 of this standard, the Safety Case for a system may depend on the Safety Cases of other sub-systems or equipment. In such circumstances, safety approval of the main system is not possible without previous Safety approval of the related sub-systems/equipment.

If Safety approval has been obtained for a generic product, or for a generic application, a reference may be made to this in the application for Safety approval of a specific application; it is not necessary to repeat the generic approval process for each application. This dependency between Safety Approvals is illustrated in figure 9.

It is essential to ensure in such examples of dependency that the Safety-Related Application Conditions stated in the Technical Safety Report of each Safety Case are fulfilled in the higher-level Safety Case, or else are carried forward into the Safety-Related Application Conditions of the higher-level Safety Case.

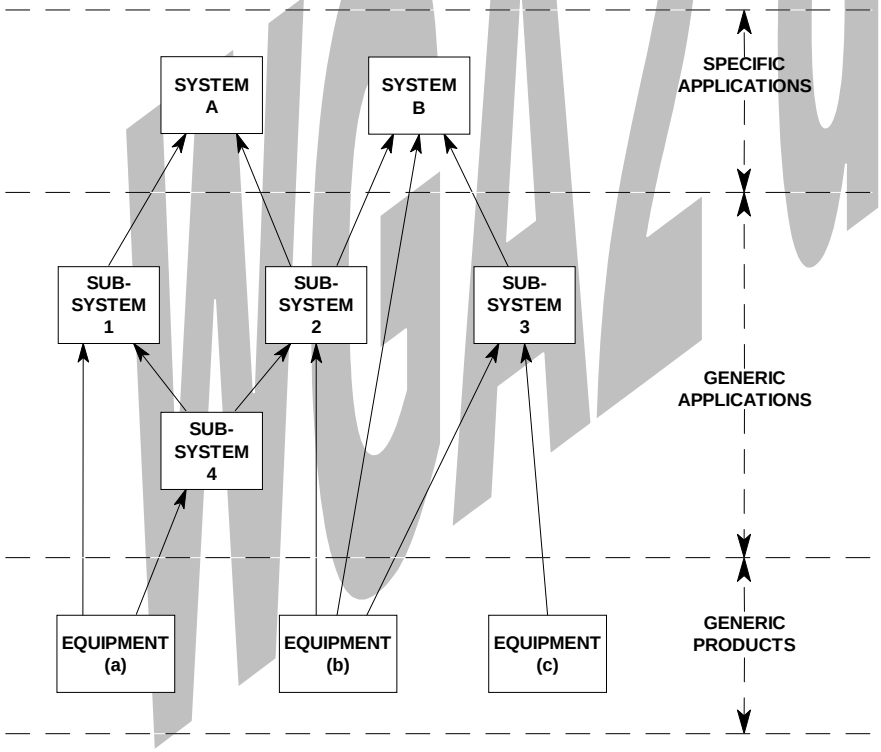


Figure 9: Safety acceptance and approval process

A Annex A (Normative) Safety Integrity Levels

A.1 Introduction

This annex defines the interpretation and use of Safety Integrity Levels in safety-related systems for railway application.

The tolerable hazard rates (THR) and quantified safety targets for each particular railway application are the responsibility of the relevant railway authority, and are not defined by this standard.

EN50126 defines the safety management process for a railway system. A life-cycle approach to safety requirements derivation and allocation shall be applied.

This includes in particular the system definition. EN 50126 already lists sufficient requirements on the definition of railway systems in phase 1 and 2 of the RAMS life-cycle.

> NOTE: Frequently, in practice the system definition is not available or well documented. The system definition is therefore a key, without which the following steps may produce incorrect or invalid results.
>
> Another important observation is that the definition of the term system depends on the perspective. The terms system, sub-system and equipment are to a great extent arbitrary. There is no fixed definition, what a system is and is not. Stated differently, the user of the process defines what the system is or is not.

A.2 Safety requirements

The system requirements specification (or sub-system/equipment as appropriate) may be considered in two parts (see figure A.1):

- Requirements which are not related to safety (including operational functional requirements);
- Requirements which are related to safety.

Requirements which are related to safety are usually called safety requirements. These may be contained in a separate safety requirements specification.

Safety requirements may be considered in two parts:

- Safety functional requirements;
- Safety integrity requirements.

Safety functional requirements are the actual safety-related functions which the system, sub-system or equipment is required to carry out.

Safety integrity requirements define the level of safety integrity required for each safety-related function.

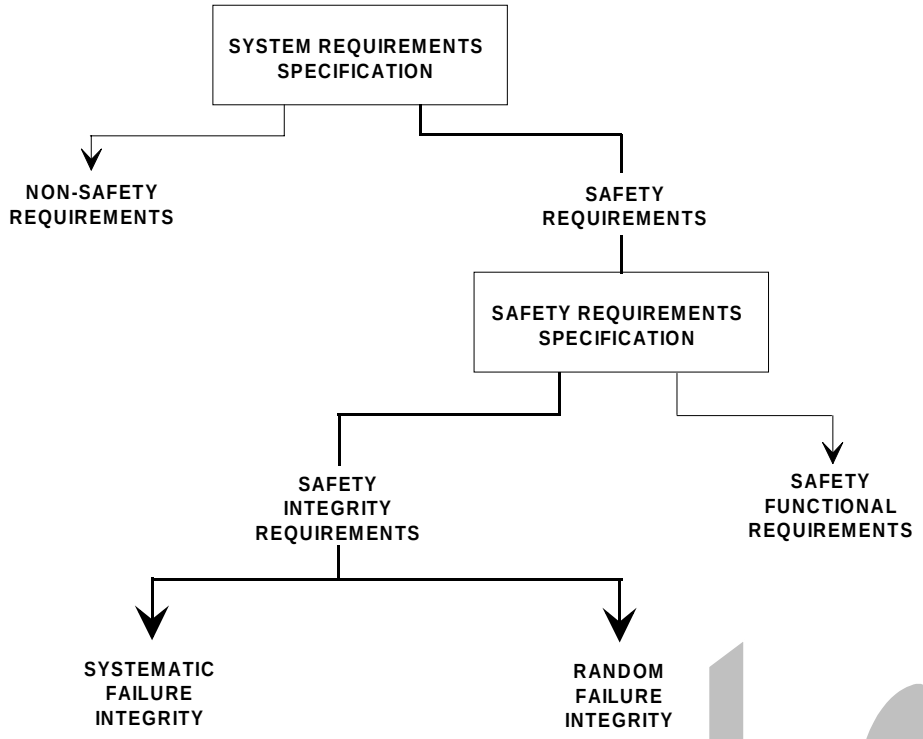


Figure A. 1: Safety requirements and safety integrity

A.3 Safety integrity

Safety integrity relates to the likelihood of a safety-related function achieving its required safety features. The higher the safety integrity of a function, the lower the likelihood that it will fail to carry out the required safety functions.

Safety integrity is comprised of two parts (see figure A.1):

- Systematic failure integrity;
- Random failure integrity.

It is necessary to satisfy both the systematic and the random failure integrity requirements if adequate safety integrity is to be achieved.

NOTE: Failures caused by environmental conditions (e.g.: EMC, temperature, vibration, etc.) should be included within systematic and random failure integrity as appropriate.

Systematic failure integrity is the non-quantifiable part of the safety integrity and relates to hazardous systematic faults (hardware or software). Systematic faults are caused by human errors in the various stages of the system/sub-system/equipment life-cycle.

FOR EXAMPLE:

- *Specification errors;*
- *Design errors;*
- *Component deficiencies;*
- *Manufacturing errors;*
- *Installation errors;*
- *Operation errors;*
- *Maintenance errors;*
- *Modification errors.*

Systematic failure integrity is achieved by means of the quality management and safety management conditions specified in sub-clauses 5.2 and 5.3 of this standard.

Technical defences against systematic faults are included in the technical safety conditions specified in sub-clause 5.4 of this standard.

Because it is not possible to assess systematic failure integrity by quantitative methods, Safety Integrity Levels are used to group methods, tools and techniques which, when used effectively, are considered to provide an appropriate level of confidence in the realisation of a system to a stated integrity level (see annex E).

Random failure integrity is that part of the safety integrity which relates to hazardous random faults, in particular random hardware faults, which are the result of the finite reliability of hardware components.

The achievement of random failure integrity is included within the technical safety conditions specified in sub-clause 5.4 of this standard.

A quantified assessment of random failure integrity shall be carried out, by means of probabilistic calculations. These are based on known data for hardware component failure rates and failure modes, and disclosure times of random hardware failures. In the case of components with inherent physical properties (see annex C) a hazardous failure rate of zero is generally assumed, although a residual risk of hazardous failure may exist and should be defended against as specified in sub-clause 5.4 and annex B.3.6 of this standard.

The global process consists of risk analysis and hazard analysis, see figure A.2. The risk analysis produces tolerable hazard rates which are the input to the hazard analysis.

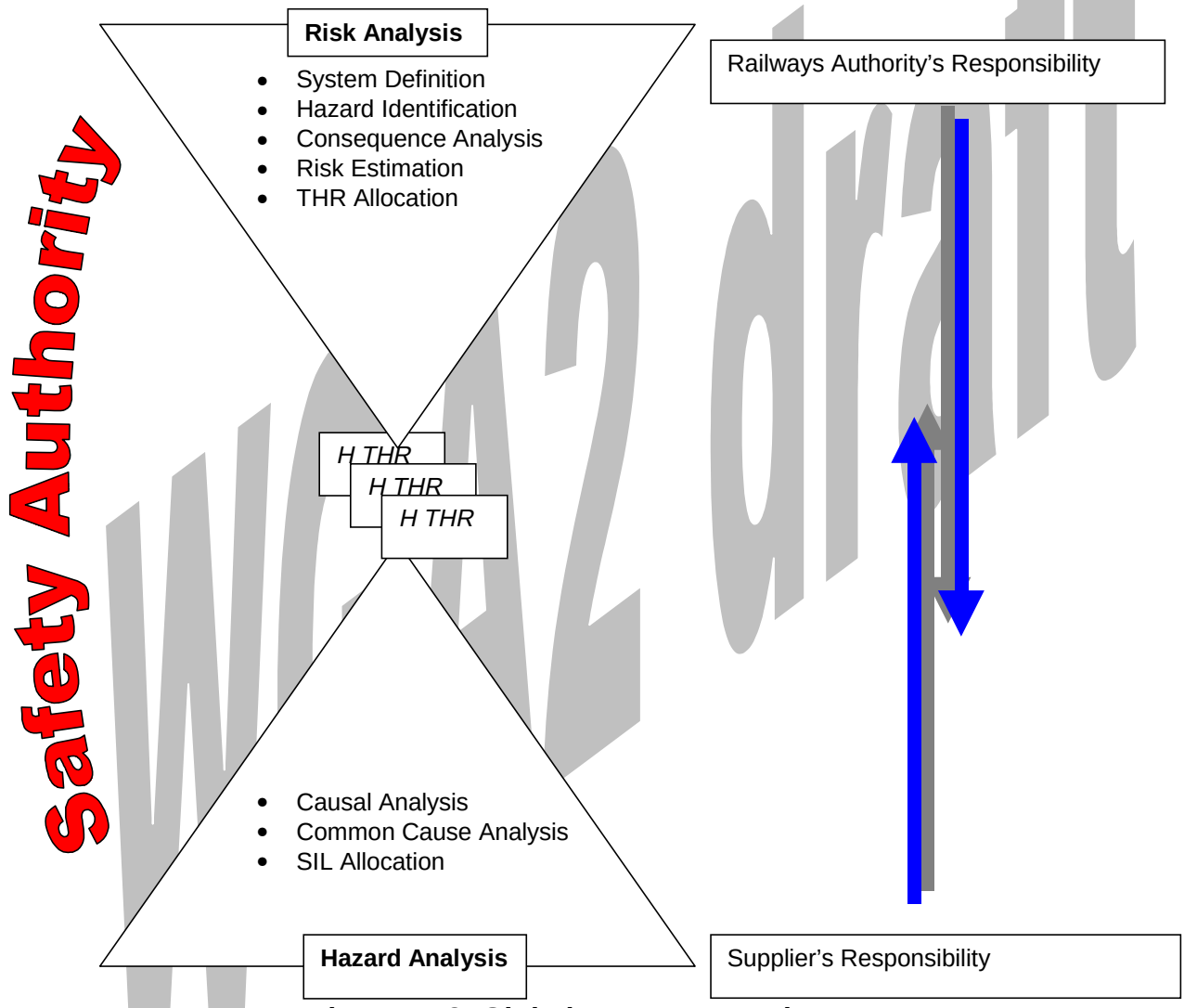


Figure A. 2: Global process overview

The safety authority shall approve both, the risk analysis and the hazard analysis.

NOTE: In some cases, these steps are not completely independent. The hazard analysis can lead to system changes which offer more safety performance. The overlapping arrows in figure A.2 show this. Hence, in these cases the global process is iterative.

The allocation of safety integrity requirements and of sfaty integrity levels are described in A.4 and A.5 respectively.

A.4 Allocation of safety integrity requirements

A methodology to determine safety integrity requirements for railway signalling equipment, taking into account both the operational environment and the architectural design of the signalling system, shall be systematically applied.

At the heart of this approach is a well defined interface between the operational environment and the signalling system. From the safety point of view this interface is defined by a list of hazards and tolerable hazard rates associated with the system. It should be noted that the purpose of this approach is not to limit co-operation between suppliers and railways authorities but to clarify responsibilities and interfaces.

From this interface the analysis proceeds as follows:

- Bottom-up analysis leads to the identification of the possible consequences of the hazards and the related risks, and
- Top-down analysis leads to the identification of the causes of the hazards.

A.4.1 Risk analysis

Figure A.3 gives a global overview of the risk analysis process. The following sections explain the phase in more detail.

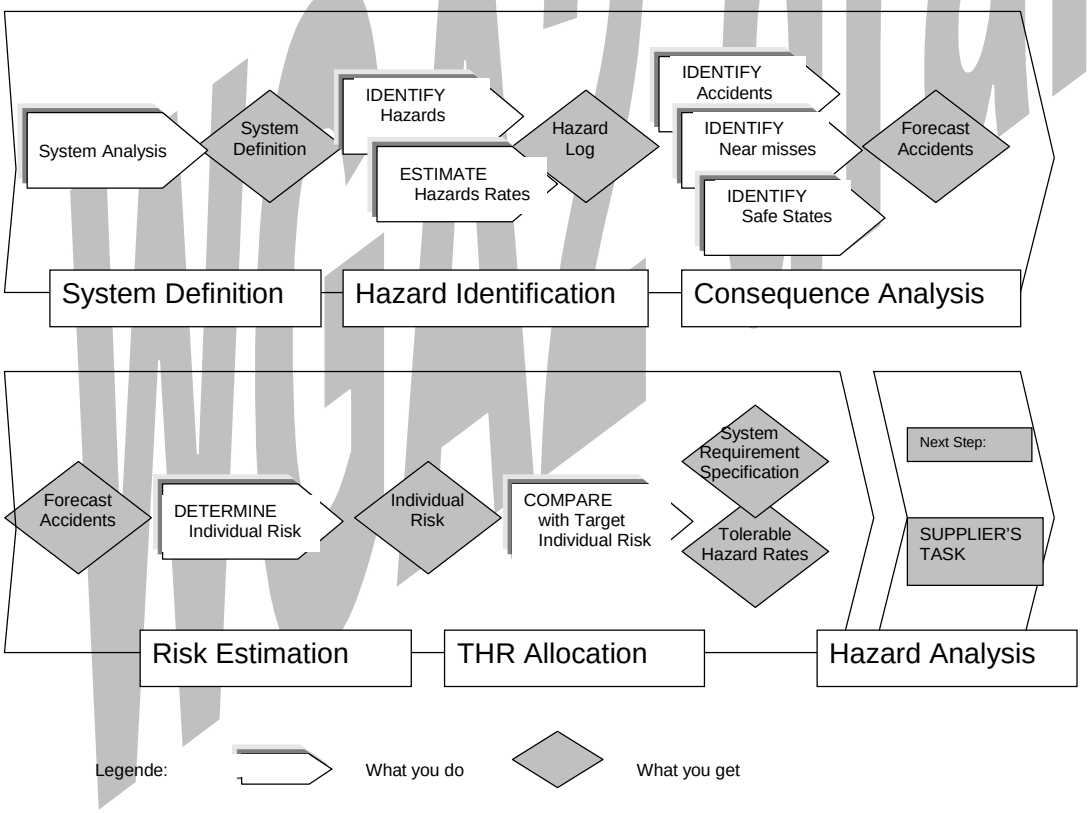


Figure A. 3: Example risk analysis process

A.4.1.1 System definition and hazard identification

It is the responsibility of the railway authority:

- To define the system (independent of the technical realisation),
- To identify the hazards relevant to the system.

Hazard identification involves systematic analysis of a product, process, system or an undertaking to determine those adverse conditions (hazards) which may arise throughout the life-cycle. Such adverse conditions may have the potential for human injury, damage to the environment or economic loss.

Systematic identification of hazards generally involves two phases:

- An empirical phase (exploiting past experience, e. g. checklists)
- A creative phase (proactive forecasting, e. g. structured what-if studies)

The empirical and creative phases of Hazard Identification complement one another, increasing confidence that the potential hazard space has been covered and that all significant hazards have been identified.

> NOTE: Methodologies which generate an unrealistically large number of mostly trivial or imprecisely defined hazards are wasteful of resource and can lead to a misleading or unproductive risk assessment. With the exception of large undertakings, involving many personnel, activities and equipment, a large list of hazards extending into the hundreds is unreasonable and indicative of a poorly designed or conducted study.

The hazards depend on the system definition and in particular the system boundary, which allows a hierarchical structuring of hazards with respect to systems and sub-systems. It also means that hazard identification and causal analysis shall be performed repeatedly at several levels of detail during the system development.

Figure A.4 shows that the cause of a hazard at system level may be considered as a hazard at sub-system level (with respect to the sub-system boundary). Thus this definition enables a structured hierarchical approach to hazard analysis and hazard tracking.

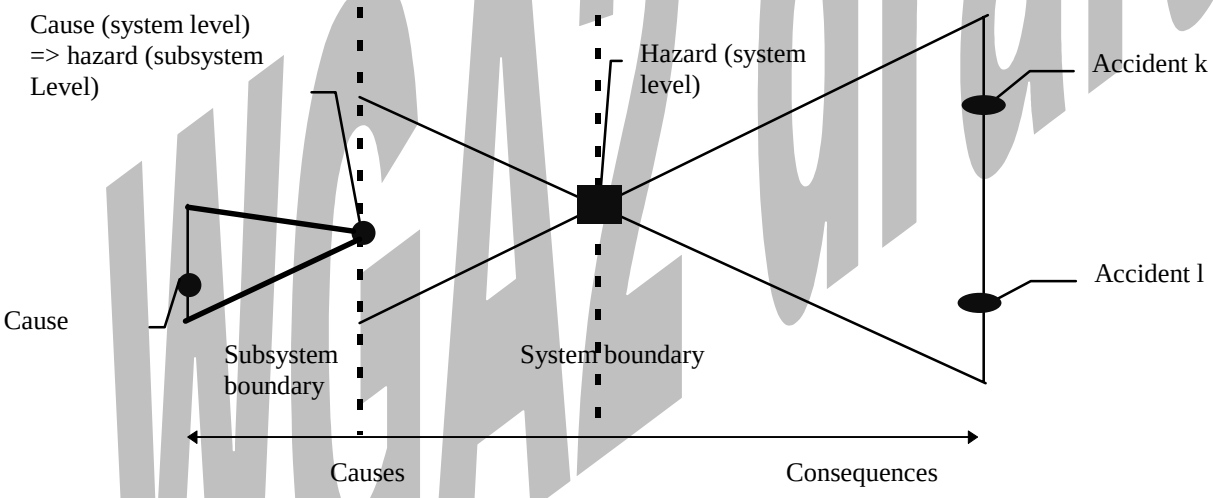


Figure A. 4: Definition of hazards with respect to the system boundary

To further ensure that risk assessment effort is focused upon the most significant hazards, the hazards should, once identified, be ordered in terms of their perceived risk level.

All identified hazards and other pertinent information shall be recorded in a Hazard Log.

A.4.1.2 Consequences analysis, risk estimation and allocation of tolerable hazards rates

It is the responsibility of the railway authority:

- To analyse the consequences, i.e. the losses,
- To define the risk tolerability criteria,
- To derive the tolerable hazard rates, and
- To ensure that the resulting risk is tolerable (with respect to the appropriate risk tolerability criteria).

The only requirement is that the resulting tolerable hazard rates shall be derived taking into account the risk tolerability criteria. Risk tolerability criteria are not defined by this standard, but depend on national or European legislative requirements.

The analysis methods shall either

- Estimate the resulting (individual) risk explicitly or
- Derive the tolerable hazard rates from a comparison with the performance of existing systems or acknowledged rules of technology, either by statistical or analytical methods, or
- Derive the tolerable hazard rates from alternative qualitative approaches, if as a result they define a list of hazards and corresponding THR.

A.4.2 Identification and treatment of new hazards arising from design

Realisation of a signalling system is likely to lead to unforeseen or undesirable properties with a potential to cause harm to people, in particular if the system or technology is new. New hazards may arise because of several aspects:

- New technology has a great potential for new hazards (lack of experience).
- Arising of an existing hidden hazard in the existing railway system due to the introduction of a new technology (e.g. analogue to digital technology).
- New design hazard due to a lack of specification.
- Special operation modes in an existing railway system may not fit well and may create new hazards for the operators, maintainers or other members of the staff, public, etc …
- Design errors may create new hazards but they can often be related to the already identified ones.

These system properties may give rise to hazardous circumstances and states which require much the same systematic treatment as applied to the hazards relating to the operational environment.

The process for identification, processing and treatment of new hazards arising from the design or application of a system is essentially identical to the risk analysis phase. Once identified, system level hazards with a potential to affect overall system performance or cause harm to people shall be declared by the supplier to the railway authority. Depending on the perceived risks, these would require qualitative or quantitative assessment, with a view to forecast and agree an appropriate tolerable rate (THR) for each.

NOTE: Then it is possible to proceed in at least two different ways:

- It is possible to relate the new hazard to an identified one: in this case the supplier should make sure that the resulting HR of the combination of these two hazards is still compliant with the THR that has been fixed by the railway authority. The hazard log and the safety case should trace this hazard.

- The new hazard has nothing to do with any of the identified ones: in this case the supplier should contact the railway authority to give him all the information he has analysed about the hazard (causes, consequences, risk, …). The railway authority should then decide whether this new hazard could be tolerated or not.
- If not, the supplier should re-design his product/system if it is possible. If not, then additional protection measures should be instigated in order to keep the risk at a tolerable level.
- If yes, then the railway authority is in charge of defining the THR of this new hazard and the supplier should provide a design compliant with this requirement.
- For both cases, once a conclusion has been reached concerning this hazard, everything shall be recorded in the hazard log and the safety case.

The THRs shall be derived for each new hazard and these will lead to updated requirements.

A.4.3 Hazard analysis

It is the responsibility of the supplier:

- To define the system architecture and allocate the system functions within the architecture (technical solution),
- To analyse the causes leading to each hazard,
- To determine the safety integrity requirements (SIL and hazard rates) for the sub-systems
- To determine the reliability requirements for the equipment

The hazard analysis process is depicted in figure A.5

A.4.3.1 Causal analysis

Causal analysis constitutes two key stages. In a first phase of the causal analysis the tolerable hazard rate for each hazard is apportioned to a functional level (system functions). The hazard rate for a function is then translated to a SIL using the SIL table. Safety Integrity Levels (SIL) are defined at this functional level for the sub-systems implementing the functionality.

A sub-system, i. e. the combination of equipment, may implement a number of safety-related functions, each of which could require different Safety Integrity Levels. Where this is the case, the sub-system shall satisfy all the required SIL levels. This can be obtained if each function meets the highest SIL or if demonstration of independence can be provided. In both cases a common cause failure analysis shall be performed.

In a second phase of the causal analysis the hazard rates for sub-systems are further apportioned leading to failure rates for the equipment, but on this physical or implementation level the SIL remains unchanged. Consequently also the software SIL defined by EN 50128 would be the same as the sub-system SIL except in the case of the exceptions described in EN 50128.

The apportionment process may be performed by any method which allows a suitable representation of the combination logic, e. g. reliability block diagrams, fault trees, binary decision diagrams, Markov models etc. In any case particular care shall be taken when independence of items is required. While in the first phase of the causal analysis functional independence is required (i. e. the failure of functions shall be independent with respect to systematic and random faults), physical independence is sufficient in the second phase (i. e. the failure of sub-systems shall be independent with respect to random faults). Assumptions made in the causal analysis shall be checked and may lead to safety-related application rules for the implementation.

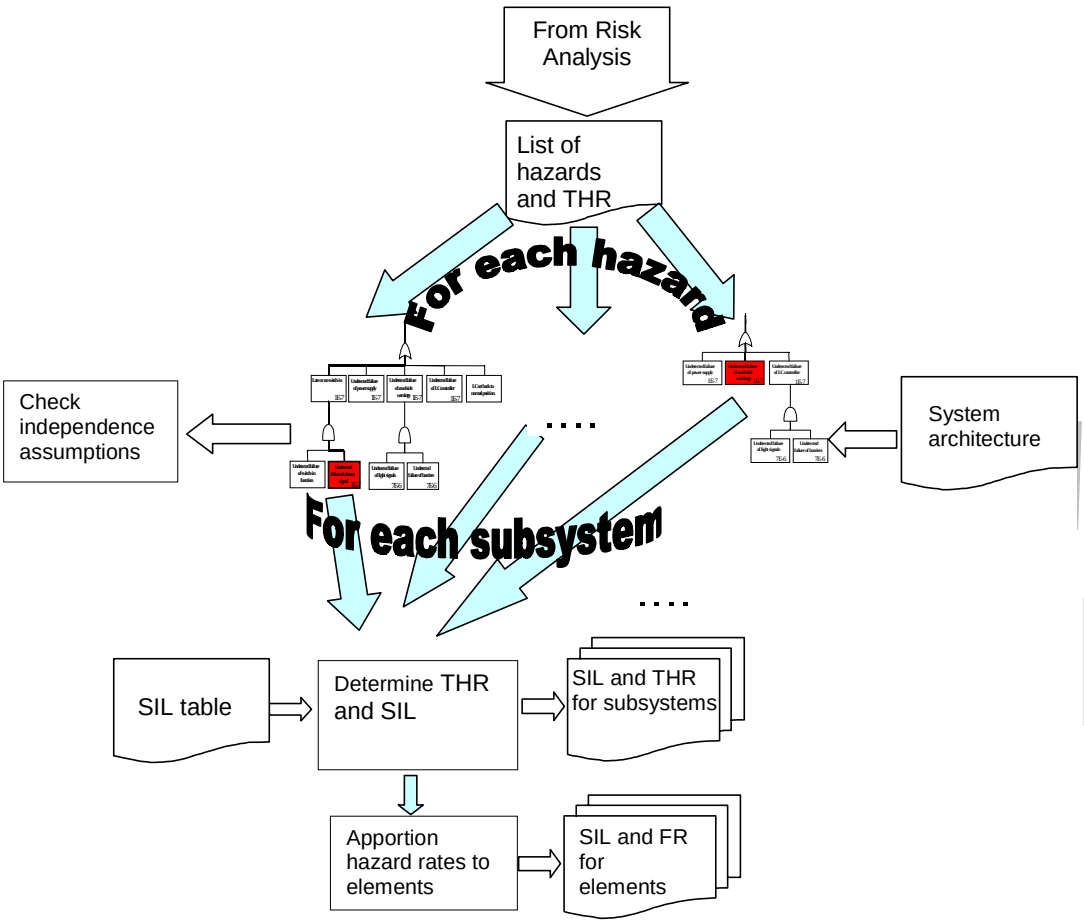


Figure A. 5: Example hazard analysis process

A.4.3.2 Common cause failure (CCF) analysis

Particular care has to be practised when independence claims (logical AND combinations) are used. It has to be ensured that sufficient

- Physical,
- Functional,
- Process

independence exists between sub-systems or system functions (see B.3.2 and B.3.6). If independence cannot be demonstrated completely then the common cause failures have to be modelled at an appropriate level of detail. Additionally it shall be demonstrated that the safety-relevant application rules immediately implied by the use of AND combinations are fulfilled and checked.

A.4.3.2.1 Physical independence

Physical independence is an absolute necessity in order to make credible fault tree calculations with AND gate for random effects. Thus in any case a common cause failure (CCF) analysis would be necessary to assume independence.

Some (informative) chapters, under which conditions for physical independence may be assumed, can be found in D.2 and D.3. A sub-chapter of the safety case also deals explicitly with *independence of items.*

NOTE: Taking a brief look at two repairable items, which are usually defined by their failure and repair rates, and a closer look at AND combinations a different interpretation of the repair rates (or equivalent repair times)

is necessary. Usually after a fault within an item has appeared, at least two things have to happen in order to get the item working again:

- The fault has to be detected and negated (this means a safe state has to be entered).
- The item has to be repaired and restored.

With repair and restore time we mean the logistic time for repair after detection, actual repair time (fault finding, repair, exchange, check) and time to restore equipment into operation. While in a reliability context usually the detection time is neglected, this time becomes important in the safety context. Safety-critical applications may not rely on self-tests or similar measures, but the detection and negation has to be performed independently of the item. Sufficient failure detection mechanisms shall be demonstrated in the safety case.

In a safety context generally the actual repair and restore time can be neglected, if other control measures are taken during this period. In this case the repair rate from reliability analysis can be interpreted as the detection and negation time, here defined as safe down time (SDT) or equivalent safe down rate (SDR).

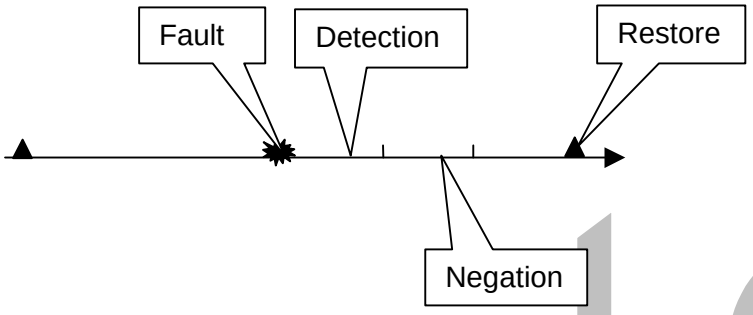


Figure A. 6: Interpretation of failure and repair times

Modelling the composition of two independent items in an AND-gate the following basic formula for the (asymptotic) tolerable hazard and detection rates for highly available systems can be used, assuming that the rates are constant over time:

$$THR_S \approx \frac{FR_A}{SDR_A} \times \frac{FR_B}{SDR_B} \times (SDR_A + SDR_B) \qquad SDR_S \approx SDR_A + SDR_B \qquad \text{(A1)}$$

where the FR's stand for Failure Rates.

If periodic testing times are used as detection times, then (A1) may be used with mean test times (T/2=1/SDR).

This means that in order to use AND combinations properly each item shall have an independent failure detection and shut-down mechanism. If an item does not have such mechanism, then according to B 3.3 of this standard the installed lifetime of the item has to be taken into account.

Another aspect, which has to be taken into account in the design, and in fact limits the free choice of parameters is the availability of the system.

Example: Taking two identical items with a MTBF of 10 000 hours and a mean detection time of 1 hour, then the resulting failure rate for the parallel system (AND combination in failure logic) is 2×10^{-8} per hour. If one item has a mean detection time of 1000 hours (e. g. detection by maintenance), then the result is only 10^{-5} per hour, which is only a factor of 10 better than the MTBF of a single item. If the mean detection time for one item would be its lifetime, then the gain would become even more marginal.

Physical independence is the lowest level of independence, typically at component level. If physical independence is assured then random integrity requirements may be apportioned to the next lower level.

A.4.3.2.2 Functional independence

Functional independence implies, that there are neither systematic nor random faults, which cause a set of functions to fail simultaneously. Thus on this level again a CCF analysis would be necessary in order to show that the functions are independent. In this standard this is called independence with respect to functional influences. Random and systematic integrity requirements may only be apportioned to the next lower level if functional independence is assured.

When applying fault tree analysis to system functions, say A and B, which is the main case in the safety integrity requirements apportionment process, it shall be taken into account that using AND gates creates immediately the following safety-relevant application rules:

- The implementations of A and B shall be physically independent.
- The safe down times defined by detection and negation times for each item shall be estimated and achieved.

Note that in general functions are not independent but can be further subdivided in independent sub-functions and sub-functions affected by CCF. Figure A.7 shows a generic treatment of CCF by FTA.

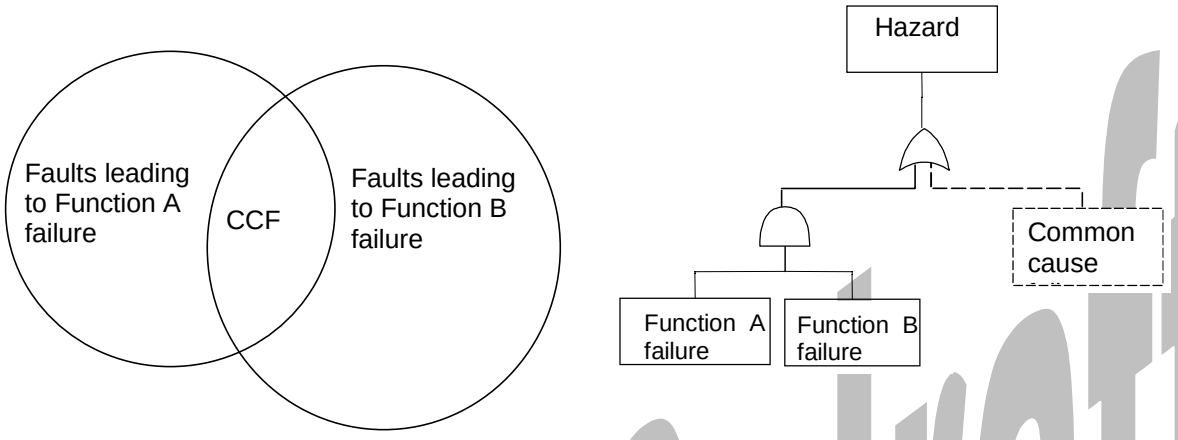


Figure A. 7: Treatment of functional independence by FTA

A.4.3.2.3 Process independence

Products and systems generally emerge as a result of activities inherent in the early life-cycle processes. These broadly comprise concept, requirements specification, system design, system development, verification and validation phases which have a significant influence on the properties of the end product. It is generally agreed that higher degrees of criticality of a product or system in its environment of application demand more robust and systematic life-cycle processes. In addition, since systematic errors inherently arise during these life-cycle processes, a degree of independence is often desirable.

In a manner similar to functional and physical counterparts, independence and diversity in human resource and life-cycle process is deemed to contribute to higher overall integrity for products and systems. Higher SIL requirements would therefore call for higher degrees of process and human resource independence to ensure systematic errors are avoided or minimised.

The development processes should fulfil the required SIL and ensure that there is sufficient organisational and personal independence between the development teams in order to further minimise systematic errors. For guidance according software issues see EN 50128.

A.5 Safety Integrity Levels

A.5.1 General aspects

Safety integrity is specified as one of four discrete levels. Level 4 has the highest level of safety integrity; level 1 has the lowest. Level 0 is used to indicate that there are no safety requirements. A SIL should address qualitative appreciation of factors such as quality and safety management (systematic failures).

Hazards related to a system are identified and assessed with regard to their potential consequences during the risk analysis phase of the system life-cycle, as described A.4.1.

This activity results (top-down) in tolerable hazard rates for each hazard. Nevertheless a supplier may start development of generic products in a bottom-up fashion and may even achieve safety approval for a generic product safety case (without the results any railway authority's risk analysis), but in the end he shall ensure that the required tolerable hazard rates (application safety case) are fulfilled. The railway authority and/or the safety authority shall determine the base line for this process.

During the next phases, the system requirements and apportionment of system requirements phases, the tolerable hazard rates are apportioned to system functions and sub-systems, respectively.

Each of these functions shall have a qualitative safety target and a quantitative target attached to them. The qualitative target shall be in the form of a Safety Integrity Level, and shall cover systematic failure integrity. The quantitative target shall be in the form of a numerical failure rate, and shall cover random failure integrity.

Safety-related functions within a system are implemented by sub-systems. Safety Integrity Levels are allocated to safety-related functions and consequently the sub-systems implementing these functions, but no further. The Safety Integrity Level for the equipment which is part of a sub-system, is the same as for the sub-system, unless functional independence can be demonstrated between equipments within sub-systems.

It is important to recognise that achievement of a specified Safety Integrity Level requires compliance with all of the factors in figure A.8, namely:

- Quality management conditions;
- Safety management conditions;
- Technical safety conditions;
- Quantified safety targets.

Fulfilment of a particular quantified safety target does not, by itself, mean that the corresponding Safety Integrity Level has been achieved. Similarly, fulfilment of the quality management, safety management and technical safety conditions associated with a particular Safety Integrity Level does not mean that the corresponding quantified safety target, or the Safety Integrity Level itself, have been achieved. All of the factors in figure A.8 need to be fulfilled in order to achieve the specified safety integrity.

It is also important to understand that, whilst the quantified safety targets in figure A.8 are those required in order to achieve the railway safety performance as described in the next paragraphs, it shall not be assumed that the target for a particular safety function can necessarily be achieved by a single *sub-system* or equipment. Where necessary the required safety target shall be achieved by combination of functions, *sub-systems* or equipment, as explained in the sections of this annex.

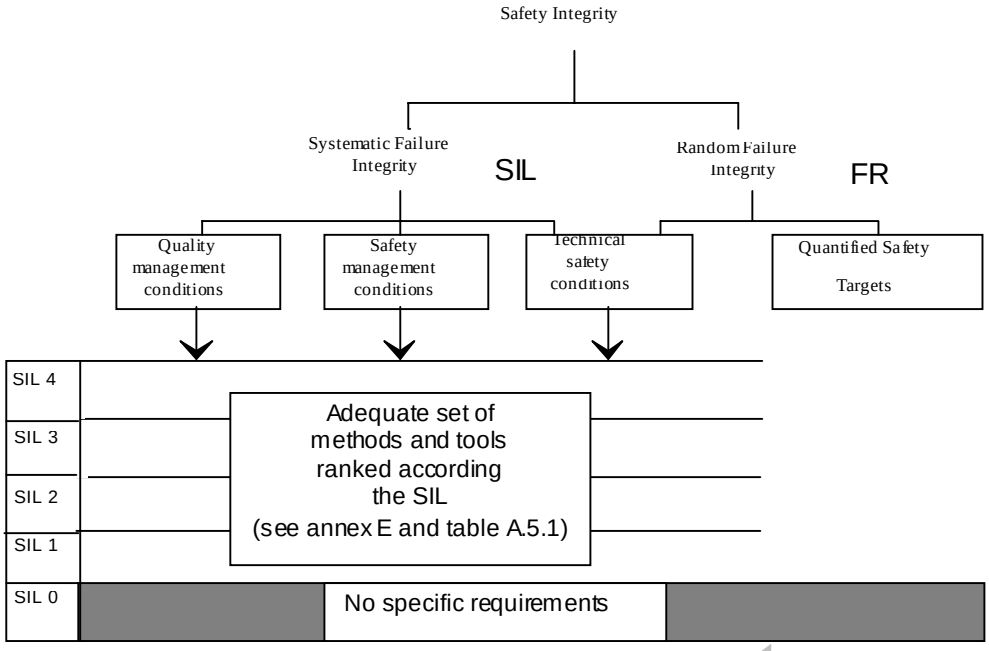


Figure A. 8: Relationship between SILs, techniques and figures

A.5.2 Relationship between SIL and safety targets

This standard is based on the assumption that safety relies both on adequate measures to avoid or tolerate faults (as safeguards against systematic failure) and on adequate measures to control random failures. Measures against both causes of failure should be balanced in order to achieve the optimum safety performance of a system. To achieve this the concept of Safety Integrity Levels (SIL) is used. SILs are used as a means of matching the qualitative approaches (to avoid systematic failures) with the quantitative approach (to control random failures), as it is agreed within CENELEC that it is not feasible to quantify systematic integrity.

Like in many other standards this balance is expressed in a table, which consists of a list of safety integrity levels 0,1,2,3,4 and a list of corresponding intervals or bands for hazard rates $I_0, \ldots, I_4$.

The SIL table is applicable to safety-related functions or *sub-system*s implementing one or more of these functions. Theoretically a SIL table should have the following properties

- Having followed the measures and methods required for SIL x (including demonstration that the failure rate is within *Ix*), the frequency of failure due to both systematic and random causes can be considered to be compliant with *Ix.* Note that for ultra-reliable systems this can only be a claim or assumption, but cannot be successfully proven.

- If for a safety-related function a hazard rate within I_x is required, then SIL *x* shall be required.

The SIL table identifies the required SIL for the safety-related function from the quantitative requirement. Thus if the THR for a function F has been derived by a quantitative method the SIL shall be determined by the use of the following table.

Table A.5.1: SIL-table

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

A function that has quantitative requirements much more demanding than $10^{-9}h^{-1}$ should not be used individually, but should be used in combination with other functions in order to achieve the necessary safety targets.

NOTE: In contrast to other standards the SIL table in this standard has only one column for frequencies (formerly called high demand or continuous mode) and does not have a column for failure probabilities on demand (formerly called demand mode). The reasons to restrict to one mode are

- Less ambiguity in determination of SIL.
- All demand mode systems can be modelled as continuous mode systems.
- Continuous control and command signalling systems are clearly the majority in modern railway signalling applications.

The SIL table has been constructed taking into account other relevant international standards.

The following shall be noted:

1. The numerical failure rates and the SIL criteria shall both be met in order to fulfil the required tolerable hazard rates.
2. The hazard rate again is defined with respect to the sub-system boundary. A hazard on this level is any undetected failure of the sub-system, which cannot be contained by the sub-system. With respect to the environment this may not necessarily be a wrong-side failure.

B Annex B (Normative) Detailed technical requirements

B.1 Introduction

As explained in sub-clause 5.4 of this standard, technical evidence for the safety of the system/sub-system/equipment design shall be presented in the Technical Safety Report (which forms Part 4 of the Safety Case). The report shall be arranged under the following headings:

Section 1. Introduction;
Section 2. Assurance of correct functional operation;
Section 3. Effects of faults;
Section 4. Operation with external influences;
Section 5. Safety-related application conditions;
Section 6. Qualification tests.

Each of these has been briefly considered in sub-clause 5.4 of this standard. More detailed requirements for sections 2 to 5 of the Technical Safety Report are contained in sections B.2 to B.5 of this annex.

The Technical Safety Report is mandatory for Safety Integrity Levels 1 to 4 inclusive (see annex A for explanation of Safety Integrity Levels). However, the depth of the information and the extent of the supporting documentation should be appropriate to the Safety Integrity Level of the system/sub-system/equipment under scrutiny. The requirements for Safety Integrity Level 0 (non-safety-related) are outside the scope of this safety standard.

The structure of the Technical Safety Report is illustrated in figure 7 of this standard.

B.2 Assurance of correct functional operation

(Section 2 of the Technical Safety Report)

This section concerns correct operation of the system/sub-system/equipment under fault-free conditions (that is, with no faults in existence), in accordance with the specified operational and safety requirements.

Some particular aspects are considered below, using the headings from sub-clause 5.4 of this standard.

B.2.1 System architecture description

This shall contain a general description of the system/sub-system/equipment design, in sufficient depth to convey a clear understanding of the principles and techniques which it uses.

B.2.2 Definition of interfaces

B.2.2.1 Man-machine interfaces

a) Operator

This shall describe the mechanisms by which the system/sub-system/equipment will be operated by operating and engineering personnel.

FOR EXAMPLE:
- *Under normal conditions;*
- *In response to alarms;*
- *By use of 'help' routines.*

b) Configuration

This shall describe the processes carried out by engineering personnel to configure the system/sub-system/equipment to a specific railway or application.

FOR EXAMPLE:
- *Software parametering;*
- *Hard wiring;*
- *Installation techniques;*
- *Procedures.*

c) Maintenance

This shall describe the interface mechanisms, including the use of any ancillary equipment, which will be used by maintenance personnel in the course of performing the various levels of maintenance.

More detailed information is contained in sub-clause B.5.2 of this annex.

B.2.2.2 System interfaces

a) Internal

This shall define the functional and physical interfaces between items internal to the system/sub-system/equipment.

FOR EXAMPLE:
- *Electrically clean and dirty areas;*
- *Internal bus structures;*
- *Communication links;*
- *Functional monitoring and correction;*
- *Diagnostic and health monitoring.*

b) External

This shall define the functional and physical interfaces between the system/sub-system/equipment and external items.

FOR EXAMPLE:
- *Sensors;*
- *Actuators;*
- *Communication links;*
- *Test and monitoring provisions;*
- *Expansion facilities.*

B.2.3 Fulfilment of system requirements specification

This shall demonstrate how the operational functional requirements specified in the system/sub-system/equipment requirements specification are fulfilled by the design. All relevant evidence shall be included (or referenced).

FOR EXAMPLE:
- *Design principles and calculations;*
- *Test specifications and results*
- *Validation*

-

B.2.4 Fulfilment of system requirements specification

This shall demonstrate how the specified safety functional requirements are fulfilled by the design. All relevant evidence shall be included (or referenced).

FOR EXAMPLE:
- *Design principles and calculations;*
- *Test specifications and results;*
- *Safety analyses and results.*

B.2.5 Assurance of correct hardware functionality

This shall describe the system/sub-system/equipment hardware architecture, and explain how the design achieves the required integrity, as laid down by the requirements specification and any relevant standards, in respect of:

- Reliability;
- Availability;
- Maintainability;
- Safety.

Consideration of safety may be limited to fault-free conditions, because effects of faults are dealt with elsewhere (see section B.3 of this annex).

B.2.6 Assurance of correct software functionality

The requirements of EN 50128 shall be complied with.

All documentation required by EN 50128 shall be included or referenced in this chapter, particularly the Software Validation Report and the Software Assessment Report.

In addition, the interaction between hardware and software shall be explained.

NOTE**:** Some particular topics which should receive attention include:
- Dependence between hardware and software;
- Sequence of interaction;
- Response times;
- Self test routines;
- Health monitoring;
- Data acquisition techniques;
- Graceful degradation;
- Negation methods.

B.3 Effects of faults

(Section 3 of the Technical Safety Report)

This section concerns the ability of the system/sub-system/equipment to continue to meet its specified safety requirements in the event of random hardware faults and, as far as reasonably practicable, systematic faults.

Particular aspects which shall be considered are detailed in sub-clauses B.3.1 to B.3.6 below, using the headings from sub-clause 5.4 of this standard.

B.3.1 Single faults

(See also guidance in table E.4)

It is necessary to ensure that the system/sub-system/equipment remains safe in the event of any kind of single random hardware fault which is recognised as possible. This principle, which is known as fail-safety, can be achieved in several different ways:

1) Composite fail-safety

With this technique, each safety-related function is performed by at least two items. Each of these items shall be independent from all others, to avoid common-mode faults. Non-restrictive activities are allowed to progress only if the necessary number of items agree. A hazardous fault in one item shall be detected and negated in sufficient time to avoid a co-incident fault in a second item.

2) Reactive fail-safety

This technique allows a safety-related function to be performed by a single item, provided its safe operation is assured by rapid detection and negation of any hazardous fault (for example, by encoding, by multiple computation and comparison, or by continual testing). Although only one item performs the actual safety-related function, the checking/testing/detection function shall be regarded as a second item, which shall be independent to avoid common-mode faults.

3) Inherent fail-safety

This technique allows a safety-related function to be performed by a single item, provided all the credible failure modes of the item are non-hazardous. Any failure mode which is claimed to be incredible (for example, because of inherent physical properties) shall be justified using the procedure defined in annex C. Inherent fail-safety may also be used for certain functions within Composite and Reactive fail-safe systems, for example to ensure independence between items, or to enforce shut-down if a hazardous fault is detected.

Whichever technique or combination of techniques is used, assurance that no single random hardware component failure mode is hazardous shall be demonstrated using appropriate structured analysis methods. The component failure modes to be considered in the analysis shall be identified using the procedures defined in annex C.

NOTE**:** A top-down failure analysis method should be used, such as Fault Tree Analysis (FTA). This should be supported, if necessary, by a bottom-up method such as Failure Modes and Effects Analysis (FMEA). See also guidance given in Table E.6.

Failure analyses shall be qualitative, and also quantitative where credible data is available. Random hardware failure rates, or probabilities of component failure, should be based on field data if possible. Apportionment of an overall component failure rate between its failure modes shall be justified in the analysis.

B.3.2 Independence of items

In systems containing more than one item whose simultaneous malfunction could be hazardous, independence between items is a mandatory precondition for safety concerning single faults. Appropriate rules or guidelines shall be fulfilled to ensure this independence. The measures taken shall be effective for the whole life-cycle of the system. In addition, the system/sub-system design shall be arranged to minimise potentially hazardous consequences of loss-of-independence caused by, for example, a systematic design fault, if it could exist.

The various types of influence in a system consisting of, for example, two operating items are represented in figure B.1. This figure may be extended to systems consisting of more than two operating items.

Where safety is reliant on the clearance and creepage distances, the minimum clearance and creepage distances shall be defined according to the application requirements (including material, technology, implementation, environmental and operation conditions, failures and temporary overvoltages).

Where safety is reliant on the clearance and creepage distances, the minimum clearance and creepage distances shall be defined according to the application requirements (including material, technology, implementation, environmental and operation conditions, failures and temporary overvoltages).

Independence could be lost by several types of influences, as explained under the following headings:

Type A Physical internal influences

If no physical connection exists between internal items of a system, there are neither physical nor functional influences. Therefore, internal independence is achieved.

NOTE**:** A physical connection is any medium between items, for example:
- galvanic connection;
- electromagnetic coupling.

Measures shall be taken to avoid non-intentional physical internal influences.

NOTE: Annex D.2 contains a range of measures for the achievement of physical internal independence (protection against influences of Type A).

Type B Functional internal influences

A functional influence between items is based on a physical connection. Measures shall be taken to avoid functional internal influences. This shall be achieved by means of functional internal independence (protection against influences of Type B).

NOTE: A functional internal influence would allow faulty information in one item to influence another item in a hazardous manner.

Type C Physical external influences

A physical external influence could cause a loss of physical independence between items.

NOTE**:** These could be due to, for example:
- environmental stresses such as EMI, ESD, climatic, mechanical and chemical;
- the power supply; and
- the external inputs and outputs.

Measures shall be taken to avoid non-intentional physical external influences.
Annex B.4 contains requirements for external influences which shall be considered.

NOTE: Annex D.3 contains a range of measures for the achievement of physical external independence (protection against influences of Type C).

Type D Functional external influences

A functional external influence could cause a loss of functional independence between items. Measures shall be taken to avoid functional external influences. This shall be achieved by means of functional external independence (protection against influences of Type D).

NOTE: A functional external influence would allow faulty information from an external source to influence the system in a hazardous manner.

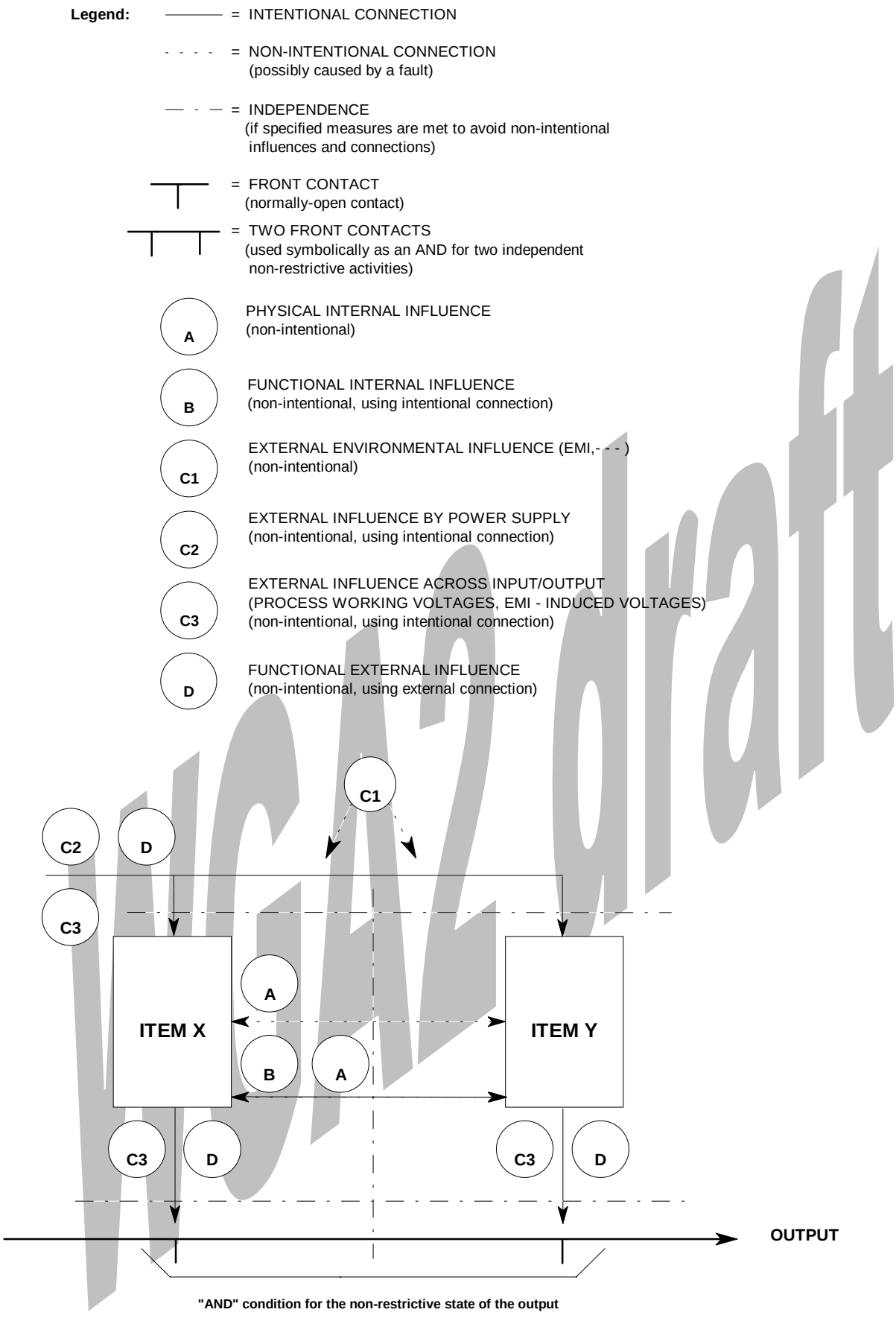


Figure B.1: Influences affecting the independence of items

B.3.3 Detection of single faults

(See also guidance given in table E.4).

A first fault (single fault) which could be hazardous, either alone or if combined with a second fault, shall be detected and a safe state enforced (i.e.: negated) in a time sufficiently short to fulfil the specified quantified safety target. Demonstration of this shall be achieved by a combination of Failure Modes and Effects Analysis (FMEA) and quantified assessment of Random Failure Integrity (see annex A.3).

In the case of Composite fail-safety, this requirement means that a first fault shall be detected, and a safe state enforced, in a time sufficiently short to ensure that the risk of a second fault occurring during the detection-plus-negation time is smaller than the specified probabilistic target.

In the case of Reactive fail-safety, this requirement means that the maximum total time taken for detection-plus-negation shall not exceed the specified limit for the duration of a transient, potentially-hazardous, condition.

These requirements for Composite and Reactive fail-safety are illustrated in figure B.2.

The techniques used to achieve detection and negation of identified faults within the permitted time shall be shown, including supporting calculations. The sources of basic failure rate data used in the calculations (for example, hardware component failure rates) shall be identified, and the method of quantitative analysis clearly explained.

> NOTE**:** The fault detection time is the test interval in the case of detection by the equipment itself, or the maintenance interval in the case of detection by staff. In the extreme case it is the installed lifetime of the system. In the case of equipment in storage, it is the interval between periodic testing by maintenance personnel.
>
> NOTE: An example of an approach to fulfilment of these requirements is contained in annex D.4.

B.3.4 Action following detection (including retention of safe state)

(See also guidance in table E.4)

After detection of a first fault, the system/sub-system/equipment shall enter, or continue in, a safe state. The safe state is generally (but not necessarily) more restrictive. The safe state shall be reached in a time sufficiently short that the combined detection-plus-negation time fulfils the specified safety target.

> NOTE: The negation time is usually the time taken for the relevant part of the system to be shut down, either automatically or by human action.

These requirements are illustrated in figure B.2.

After detection of a first fault, and having entered the safe state, further faults shall not cancel out the safe state. Cancellation of a restrictive safe state shall occur only in a controlled manner, as part of a corrective procedure.

The system/sub-system/equipment shall remain in a safe state if further faults occur during permissible delay-times-to-repair after occurrence of a first fault. Permissible delay-times-to-repair shall be sufficiently short to fulfil the specified safety target.

B.3.5 Multiple faults

(See also guidance given in table E.4).

A multiple fault (for example, a double or triple fault) which could be hazardous, either directly or if combined with a further fault, shall be detected and a safe state enforced (i.e.: negated) in a time sufficiently short to fulfil the specified safety target. A suitable method, for example Fault Tree Analysis (FTA), shall be used to demonstrate the effects of multiple faults. The techniques used to achieve detection-plus-negation of multiple faults within the permitted time shall be shown, including supporting calculations.

> NOTE: An example of an approach to fulfilment of these requirements is contained in annex D.5.

A Common-Cause Failure (CCF) analysis shall be carried out, to provide assurance that a multiple fault could only occur by means of a combination of random single faults, and not as the result of a common-cause fault.

B.3.6 Defence against systematic faults

In addition to the quality and safety management techniques which are used to minimise the probability of human error (see sub-clauses 5.2 and 5.3 of this standard), technical measures shall be taken such that if a hazardous systematic fault should exist it would, as far as reasonably practicable, be prevented from creating an unacceptable risk.

> *FOR EXAMPLE: The architecture of the overall system could be configured such that, even in the event of a hazardous failure of a sub-system or item of equipment which has been designed to be safe, an accident would still be unlikely to occur.*

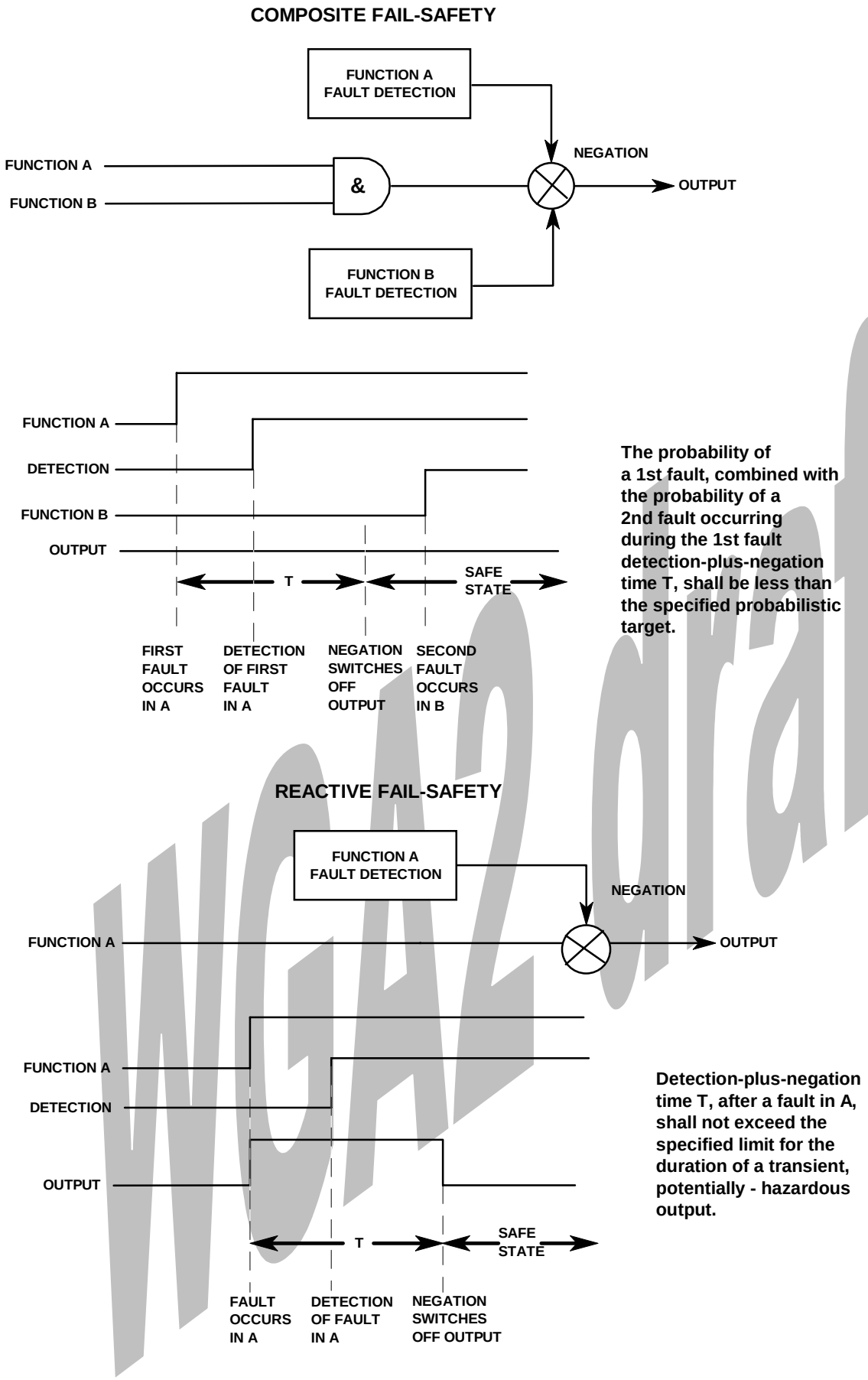


Figure B.2: Detection and negation of single faults

B.4 Operation with external influences

(Section 4 of the Technical Safety Report)

This section concerns the ability of the system/sub-system/equipment to operate correctly and safely when subjected to specified external influences. "Correct operation" includes fulfilment of both operational and safety requirements.

As far as reasonably practicable, safety-related systems should be designed to remain safe even if subjected to external influences outside the specified limits.

The influences which shall be considered are listed in sub-clauses B.4.1 to B.4.7 below. The values for different conditions listed in EN 50125-1 and EN 50125-3 shall be complied with.

Consideration shall be given to the effects of storage and transportation.

B.4.1 Climatic conditions

It shall be ensured that under the specified climatic environmental conditions, which shall be taken from EN 50125-3, safety to the required European standards is achieved.

If the railway authority specifies more severe conditions than the equipment can fulfil the supplier can, in agreement with the customer, add measures for climatisation.

B.4.2 Mechanical conditions

It shall be ensured that under the specified mechanical environmental conditions, safety to the required European standards is achieved.

B.4.3 Altitude

It shall be ensured that at the actually occurring altitude, safety to the required European standards is achieved.

NOTE: The altitude at which the system/sub-system/equipment is to function does not normally exceed 1800 metres above sea level.

B.4.4 Electrical conditions (not on vehicles)

It shall be ensured that under the specified electrical environmental conditions, safety to the required European standards is achieved.

NOTE: The values quoted in EN 50121-4 and EN 50124-1 should be used as a basis.

B.4.5 Electrical conditions (on vehicles)

It shall be ensured that under the specified electrical environmental conditions on vehicles, safety to the required European standards is achieved.

NOTE: The values quoted in EN 50121-3, EN 50124-1 and EN 50155 should be used as a basis.

B.4.6 Protection against unauthorised access

1) Definition of access levels

The access level defines who has access, reason for access and how access is achieved, thereby guarding against unauthorised access. For each of the particular operations below, persons performing these functions will require to meet certain criteria, which shall be defined in respect of:

- Skill discipline;
- Skill level;
- Equipment-specific training.

2) Protection

With respect to the above access levels, this section shall define how protection is to be achieved.

The protective measures should guard against access which is:

- Accidental, by authorised persons;
- Intentional, by unauthorised persons.

3) External conditions

This shall describe how protection is achieved by means additional to the equipment itself.

FOR EXAMPLE:
- *Housing;*
- *Security;*
- *Accessibility.*

4) Encapsulation

This shall describe how protection is achieved by the actual equipment.

FOR EXAMPLE:
- *Covers;*
- *Mounting;*
- *Seals;*
- *Coding, electrical;*
- *Coding, mechanical;*
- *Firmware.*

B.4.7 More severe conditions

Where necessary, provision shall be made to deal with additional, more severe, conditions specified by the railway authority.

NOTE: The following are examples of more severe conditions:
- Condensation due to rapid variation in ambient temperatures of equipment;
- Severe pollution of the air by:
- Dust;
- Smoke;
- Steam;
- Corrosive chemicals;
- Salt;
- Hydrogen sulphide;
- Etc.

The kinds of pollutants and their concentration should be defined in the specification.

For outdoor equipment:
- Frost;
- Rapid temperature change;
- Chemical influences such as:
- Oil products;
- Organic elements;
- Weed killers;
- Excessive heating from, for example, fire or solar radiation;
- Action/entry of plants, insects or animals;
- Accumulation of dirt and dust (conductive and/or non-conductive);
- More extreme temperature limits in some countries.

B.5 Safety-related application conditions

(Section 5 of the Technical Safety Report)

This section shall define the rules, conditions and constraints relevant to functional safety which need to be observed in the application of the system/sub-system/equipment.

- General topics which shall be considered include the following:
- Configuration of programmable systems to suit specific applications;
- Precautions in manufacturing, installation, testing and commissioning;
- Rules and methods for maintenance and fault-finding;
- Instructions for system operation;
- Safety warnings and precautions;
- Electromagnetic compatibility (EMC) precautions (susceptibility and emission);
- Information concerning modifications and eventual de-commissioning;
- Safety justification of support equipment and tools, such as test equipment, maintenance equipment and configuration tools.

Some specific topics which shall be included are listed in sub-clauses B.5.1 to B.5.3 below.

B.5.1 Sub-system/equipment configuration and system build

1) Configuration

If a sub-system or equipment is such that it has to be configured for each particular application, then any configuration tools and/or procedures shall be defined.

FOR EXAMPLE:
- *Procedural methods;*
- *Version control;*
- *Hardware requirements of configuration system;*
- *Software details of configuration system;*
- *Software maintenance;*
- *Verification and validation;*
- *Simulation.*

2) System build

This documentation shall detail how sub-systems and equipment are built into a particular signalling system.

FOR EXAMPLE:
- *Version control settings;*
- *Application control settings;*
- *Interface settings;*
- *Initialisation settings;*
- *Maintenance control settings;*
- *Manufacturing and production testing;*
- *System test routines;*
- *Installation, testing and commissioning.*

3) Change of functionality

If a sub-system or equipment is of sufficient generic design that it could be employed in systems for various applications, then how it is configured and set-up to meet these different applications shall also be documented. Any limitations or conditions for safe use shall be fully specified.

B.5.2 Operation and Maintenance

The necessary minimum maintenance to ensure continued safe and correct operation of the system/sub-system/equipment within the specified environmental conditions shall be documented in the form of an Operation and Maintenance Plan, which shall include the following aspects:

1) Operational status

The conditions that exist in each system/sub-system/equipment shall be defined to provide operating and maintenance personnel with sufficient understanding during the following situations:

a) Start-up

This shall describe the start-up conditions of the system, sub-system or equipment when power is initially applied, or following shut-down due to power interruption or other cause.

NOTE: This should define, for example:
- Default conditions;
- Initialisation period;
- Self checks performed;
- Manual intervention required;
- Condition of outputs;
- Precautions after an exceptional event, such as fire or unauthorised entry.

b) Normal operation

Once the system/sub-system/equipment has successfully completed initialisation, the conditions during normal operation shall be defined.

FOR EXAMPLE:
- *Cycle times;*
- *Non-data routines;*
- *Disclosure of faults.*

c) Changeover

If the equipment, or the system/sub-system in which it is configured, has a facility to change over to either a cold or hot standby system/sub-system, then the conditions defined in a) and b) shall be re-stated for this changeover routine. The reaction of the equipment to the changing of failed modules shall also be clearly defined.

d) Shut-down

When a system, sub-system or item of equipment is shut down intentionally for a configuration change or de-commissioning, or unintentionally via a power failure, then all relevant conditions shall be defined.

FOR EXAMPLE:
- *Default conditions;*
- *Conditions for graceful degradation;*
- *Safety aspects;*
- *Procedures;*
- *Influences on other connected systems.*

2) Maintenance levels

These shall be defined in respect of:

- First line maintenance;
- Second line maintenance by customer;
- Second line maintenance by manufacturer.

NOTE: "First line" is preventative maintenance and fault-finding/repair carried out on site, with "second line" being preventative maintenance and possible repair in a workshop environment, that is, off site.

3) Periodic maintenance

In describing the periodic maintenance required, reference shall be made to all relevant areas.

FOR EXAMPLE:
- *Training;*
- *Accessibility;*
- *Modularity;*
- *Interchangeability;*
- *Spares provisions;*
- *Storage of spares.*

4) Maintenance aids

For each level of maintenance, the maintenance aids available to personnel shall be defined.

NOTE: These aids should include, for example:
- Fault diagnostics;
- Interpretation of fault messages;
- Fault correction.

B.5.3 Operational safety monitoring

During the operation and maintenance phase of the system life-cycle, the performance of the system/sub-system/equipment shall be monitored to ensure that the features incorporated into the design, and the assumptions made during the initial safety assessment, remain valid for the actual circumstances encountered during in-service use.

NOTE**:** This should include, for example:

- The monitoring of safety-related performance and comparison with the predicted performance;
- The monitoring and assessment of failure reports to detect failure trends or possible hazardous failures which can be corrected, thereby improving safety and reliability;
- Investigation of incident and accident reports to identify any changes required to improve the safety performance of the system.

B.5.4 Decommissioning and disposal

The technical safety precautions and procedures which will be necessary when the system/sub-system/equipment is eventually decommissioned shall be documented. This shall include consideration of possible phased introduction of replacement systems whilst the railway continues in operation.

Appropriate warnings and instructions concerning final disposal of equipment after decommissioning shall also be included.

B.6 Safety Qualification Tests

(Section 6 of the Technical Safety Report)

This section shall contain evidence to demonstrate successful completion of the Safety Qualification Tests under operational conditions.

The purpose of these tests is:

- To gain increased confidence that the system/sub-system/equipment fulfils its specified operational requirements;
- To gain increased confidence that the specified reliability and safety targets have been achieved;
- To allow systems/sub-systems/equipment to be put into operational service before final Safety Approval, subject to provision of appropriate precautions and monitoring.

NOTE: These tests only provide increased confidence and are not the unique means for demonstration of safety.

B.6.1 Requirements

The extent and duration of the Safety Qualification Tests shall be agreed between the railway authority and the safety authority, and shall be justified having regard to the degree of novelty and complexity associated with the system/sub-system/equipment.

Because completion of the Safety Qualification Tests is contained within the Safety Case, the safety of the system is not fully assured during the test period. Therefore appropriate precautions, procedures and monitoring shall be provided, to ensure safety of the railway during the test period.

Safety Qualification Tests, as defined, shall be completed before commencing operation with full responsibility for safety.

A record shall be established which explains when the system is put into service, with or without passengers, with or without precautions, and what is the authorisation level obtained at each stage (provisional or final Safety Approval).

B.6.2 Results

An account of the Safety Qualification Tests, including a full description of the tests carried out and the results obtained, shall be documented in this section of the Technical Safety Report.

C Annex C (Normative) Identification of hardware component failure modes

C.1 Introduction

This annex contains procedures and information for identifying the credible failure modes of hardware components.

NOTE: The tables of hardware component failure modes included in this annex have been derived from European experience and also from the following sources listed in annex F (informative):

- UIC/ORE Report A155/RP12
- MIL-HDBK-338-1A
- German Federal Railways Mü8004
- Reliability Analysis Center Report FMD-91

The information in the tables may be modified, as explained in sections C.2 and C.5 of this annex, if adequate justification is provided for such variations.

C.2 General procedure

For the purpose of analysing the results of single faults (see annex B.3.1), it is necessary to identify the credible failure modes of each hardware component.

Tables C.1 to C.16 contain lists of hardware component failure modes which shall be used as the basis for design and analysis, unless justification is provided for any variation. The general notes in section C.5 of this annex shall be observed.

The lists are not necessarily complete, and any additional failure modes which are considered to be credible shall be added to the analysis. In such cases, the extra failure modes should be drawn to the attention of the relevant authority, so that the lists can be extended at a future date, by means of the normal CENELEC procedure.

C.3 Procedure for integrated circuits (including microprocessors)

Designs which employ integrated circuits require special treatment, since it can be difficult to predict all the credible failure modes that the device may possess. This is particularly true for programmable devices, since the failure modes that may be observed at the boundary of the device are application specific.

It is recommended that the hazardous failure modes be identified in a top-down manner for the specific application, using a technique such as Fault Tree Analysis. (An alternative would be to use a bottom-up approach such as Failure Modes and Effects Analysis, but this method is time-consuming and it is possible that certain hazardous failure modes could be missed).

As assessment and justification shall then be made, to show that for each identified hazardous failure mode:

either a) The failure mode cannot credibly occur, due to the internal software architecture or data structure;

or b) The failure mode will be externally detected and a safe state imposed within the required time. In this case, quantitative analysis should be performed to justify the design, and a pessimistic view should be taken whereby the hazardous failure modes are assumed to take the full component failure rate.

NOTE: Some items, such as "intelligent" sensors, employ embedded microprocessors. Such items should be assessed using the same methods as outlined above for integrated circuits.

C.4 Procedure for components with inherent physical properties

If the technique of Inherent Fail-Safety is used (see annex B.3.1), full justification shall be provided for any component failure mode which is considered to be incredible. This justification shall include, but not necessarily be limited to, the following topics:

- Theoretical explanation of inherent physical properties;
- Evidence of compliance with recognised quality standards;
- Explanation of special construction of components;
- Explanation of special mounting arrangements or other precautions for the component;
- Evidence that the failure mode will not occur as a result of component ratings being exceeded (for example, because of fault or overload conditions);
- Results of tests to demonstrate fail-safe behaviour of component under adverse conditions;
- Evidence of previous experience of reliance on the component for inherent fail-safety.

If satisfactory justification is provided, the relevant component failure modes may be excluded from the safety analysis.

It is not necessary to repeat the justification if it has already been provided in the past; it is sufficient to make reference to the previous justification report. However, if this justification includes particular conditions (for example, special mounting arrangements or means for prevention of overload), the fulfilment of these conditions shall be included in the Safety Case.

Previous experience indicates that some particular component failure modes are more likely to be capable of justification as incredible; these failure modes are indicated by **(*)** in tables C.1 to C.16, together with relevant guidance notes in sections C.6 and C.7 of this annex. Other component failure modes are much less likely to be capable of justification as incredible. Note that justification shall be provided for all failure modes which are considered to be incredible, including those which are indicated in the tables.

C.5 General notes concerning component failure modes

(a) Tables C.1 to C.16 contain lists of credible failure modes of hardware components.

(b) The failure modes are as manifested at the boundary of the components, and not the internal physical causes of the failures.

(c) All listed failure modes could be intermittent.

(d) Intermittent failures are caused by environmental influences such as temperature variation or mechanical stress. Therefore the frequency of intermittent failures will be in accordance with these reasons.

(e) Variations within the tolerances of a component's published specification are not considered to be failures.

(f) It is assumed that components are operated within their published environmental limits.

(g) It is assumed that components are operated within their published electrical ratings.

(h) External short-circuit or leakage between terminals of a component is not considered to be a component failure. For suitable creepage and clearance distances, which

have to be dimensioned in accordance with the requirements for re-inforced insulation, refer to EN 50124-1.

(i) External short-circuit or leakage between different components is not considered to be a component failure. For suitable creepage and clearance distances, which have to be dimensioned in accordance with the requirements for re-inforced insulation, refer to EN 50124-1. Stable mounting and/or special fastening will be necessary if environmental conditions could change the position of a component.

C.6 Additional general notes, concerning components with inherent physical properties

(1) The procedure and conditions for justification of any component failure mode as incredible are contained in section C.4 of this annex.

(2) Failure modes indicated by **(*)** in tables C.1 to C.16 are those which are more likely to be capable of being justified as incredible.

(3) "Note xy" following **(*)** in tables C.1 to C.16 refers to guidance notes in section C.7 of this annex on some factors that are relevant to possible justification of the failure mode as incredible.

(4) The general notes in section C.5 of this annex apply also to components with inherent physical properties, with the following additions in notes 5, 6 and 7 below.

(5) In addition to note (e) in section C.5, it is recommended that some allowance be made for variations which exceed the normal tolerances.

(6) In addition to note (f) in section C.5, it is recommended that some allowance be made for excursions beyond the normal environmental limits.

(7) In addition to note (g) in section C.5, a margin shall be ensured within the published electrical ratings, so that the component is protected from being overloaded.

(8) Not used.

(9) Not used.

C.7 Specific notes concerning components with inherent physical properties

The following notes provide guidance concerning possible justification of the failure modes identified by **(*)** in tables C.1 to C.16 as incredible.

(10) The body should have no hollows.

Clearance and creepage distances between the caps/connection wires at each end of the component should at least fulfil the requirements of EN 50124-1, in accordance with its requirements for re-inforced insulation.

The winding of a wire-wound resistor should have only one layer.

The component should be coated with cement or enamel.

Short-circuit between turns of a wire-wound resistor should be avoided by coating of the wire, and/or by physical separation of the turns.

The body should be constructed of material which is non-conductive, even at the highest temperature (including fault conditions).

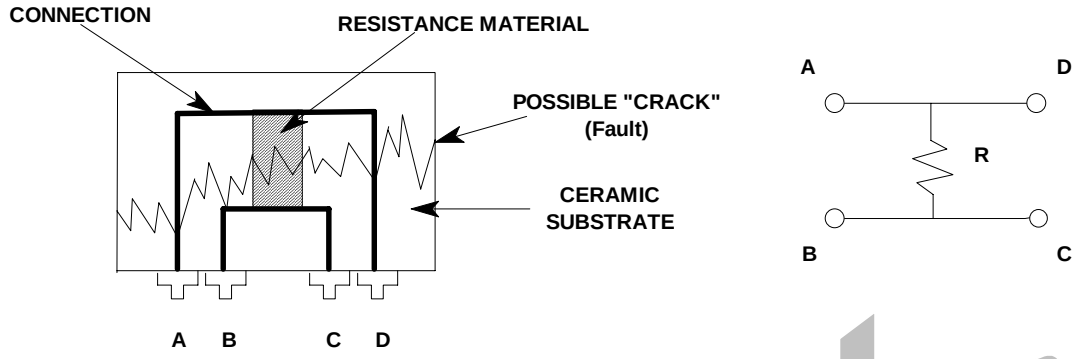
The coating should be non-conductive, even at the highest temperature (including fault conditions).

The resistance should be limited to the lowest possible value (for example, no greater than 10k Ω).

(11) The 4-terminal resistor should be constructed in such a way that, if a fault causing interruption of the resistance material occurs, this fault would also cause interruption of at least one of the four connecting terminals.

The circuitry external to the resistor should disclose the interruption of the terminal(s) in a fail-safe manner.

Example of a 4-terminal resistor, using a hybrid thick layer technique:



(12) Two terminals should be connected independently to each side of the component.

(13) The formula to calculate capacitance of a simple parallel-plate capacitor is:

$$C = \varepsilon_0 \cdot \varepsilon_r \cdot \frac{A}{d}$$

where A = common area of plates;
d = distance between plates;
ε_0 = permittivity of free space;
ε_r = relative permittivity (dielectric constant).

Justification of the failure mode as incredible requires demonstration that none of these parameters can significantly change.

Electrolytic capacitors are not suitable for exclusion from this failure mode.

(14) The capacitor should be designed and constructed for high-voltage application in relation to the maximum possible operating voltage (including fault conditions). It should have Class-Y specification, and self-healing properties at the working source impedance and over the working voltage range.

(15) There should be only one layer of turns, separated by means of grooves in the insulated body, or the wire should have re-inforced insulation.

The turns should be securely fastened.

(16) Clearance and creepage distances should fulfil at least the requirements for re-inforced insulation of EN 50124-1.

All windings and connections should be securely fastened.

Power dissipation should be limited sufficiently to prevent internal carbonisation (including fault conditions).

(17) The magnetic core should be constructed such that no significant change in reluctance of the magnetic path can occur.

(18) The transfer ratio depends upon the number of turns on each winding, and on the integrity of the magnetic coupling. Therefore it is necessary for notes (15), (16) and (17) to be fulfilled.

(19) The transductance and the d.c. threshold voltage depend upon the properties of the magnetic core material. Therefore it is necessary to demonstrate that these magnetic properties cannot significantly change.

Transductance and d.c. threshold voltage also depend on the number of turns on each winding, and on the integrity of the magnetic coupling. Therefore it is also necessary for notes (15), (16) and (17) to be fulfilled.

The output from a transductor is related to the number of ampère-turns in the control winding. It is necessary to demonstrate that, in conjunction with the associated drive circuitry, no credible failure modes of the control winding can cause an increase in the number of ampère-turns.

(20) All parts of the relay or switch mechanism should be robustly constructed and securely fastened, including:

- the operating mechanism;
- the contact system;
- the magnetic circuit (if any);
- the coil(s) (if any).

Clearance and creepage distances should fulfil at least the requirements for re-inforced insulation of EN 50124-1.

(21) Contact materials should be chosen which are not capable of being welded.

The risk of welding should be further reduced by appropriate mechanical design and construction of the contacts.

The maximum current should be limited, to ensure that the temperature of the contacts does not reach a value at which welding could occur.

(22) Stability of the relay's characteristics should be ensured by careful attention to the following factors:

Magnetic characteristics

- Choice of magnetic material;
- Provision of a stop device to avoid permanent magnetisation of the magnetic circuit (core);
- Protection against external magnetic fields;

Electrical characteristics

- Choice and quality of the wire and insulation;
- Quality of winding of the coil;
- Quality of terminations;

Mechanical characteristics

- Choice and quality of materials;
- Secure fastening of all parts;
- Secure retention of all safety-related adjustments;
- Provision of adequate return force, using gravity (supplemented
- if necessary, by springs and/or by elasticity of blades);
- Design and construction of the operating mechanism such that it cannot become jammed.

(23) The threshold voltage of a p-n junction, such as a diode or a transistor base-emitter junction, is a function of:

- Minority and majority charge-carrier densities;
- Boltzmann's constant (k);

- Electron charge (e);
- Temperature (K).

Therefore the threshold voltage is dependent on non-variable characteristics of the p-n junction, and should be constant for a given temperature.

(24) The breakdown voltage is determined by one of two possible mechanisms: Zener breakdown or avalanche breakdown. Both of these are dependent on non-variable physical characteristics of the diode, so the breakdown voltage should be constant for a given temperature.

Care should be taken to avoid components which consist internally of two or more diodes connected in series.

Note that conduction at voltages above and below the breakdown voltage may be possible, due to shunt or series resistance, but the differential (slope) resistance in such cases would be higher than for the case of breakdown conduction.

(25) The amplification (or gain, or transconductance) of a transistor, and the optical sensitivity of a photo-diode or transistor, are dependent on:

- Doping levels;
- Thickness of the junction(s);
- Life-time of charge carriers.

These parameters should remain constant, with the exception of the charge carriers' life-time, which can only decrease with time. Therefore the amplification/sensitivity should remain constant, or possibly decrease, but not increase.

A small possibility exists of an increase in amplification caused by pollution affecting surface doping. This can be avoided by high-quality manufacture and packaging of the component. Also this effect is only significant for very low bias currents, which should therefore be avoided when designing circuits.

(26) Light emission is a physical property related to recombination of electrons and holes when current flows in a forward-biased p-n junction.

The rate of recombination is a function of the forward current, and therefore the light emission should not increase at constant current.

Below the threshold voltage there is no significant current flow and therefore no light emission.

(27) If the p-n junction is reverse biased, there will be no significant current flow below the breakdown voltage and therefore no light emission.

Above the breakdown voltage, the mechanism that allows current to flow is different to that for forward bias and should not result in emission of light.

(28) For optocouplers and self-contained fibre-optic systems, the failure modes of each element should be considered, i.e.:

- Light-emitting transmitter;
- Optical medium;
- Photo-sensitive receiver.

(29) Clearance and creepage distances should fulfil at least the requirements for re-inforced insulation of EN 50124-1.

The construction of the components should be robust and stable.

Power dissipation in the component should be limited sufficiently to prevent internal carbonisation (including fault conditions).

(30) Clearance and creepage distances should fulfil at least the requirements for re-inforced insulation of EN 50124-1.

The input and output drive/coupling elements should be securely fastened.

(31) The component should be robustly constructed.

The resonator(s) should be constructed and mounted so as to prevent change of their effective dimensions.

The resonator(s) should be constructed of a material whose dimensions are not significantly altered by changes of temperature.

The material of the resonator(s) should be stabilised by temperature cycling and/or pre-operation for a sufficient time.

The material of the resonator(s) should not be over-stressed, even under fault conditions. In particular the limit of elasticity should not be exceeded.

(32) The transfer ratio is a function of the efficiency of the drive/coupling elements and the Q-factor of the filter.

The drive/coupling elements should be designed and constructed so as to prevent any significant increase in their efficiency.

(33) The resonator(s) should be constructed and mounted to obtain the maximum possible Q-factor, so that no subsequent improvement can occur.

(34) The resonator(s) should be constructed and mounted so as to prevent the occurrence of damping by any mechanism.

(35) The insulating material should be stable.

Clearance and creepage distances should fulfil at least the requirements for re-inforced insulation of EN 50124-1.

(36) The connector should be robustly constructed.

All parts of the connector should be securely fastened.

(37) Incorrect orientation of the connector, or insertion into the wrong socket, should be prevented by means of, for example, mechanical design or mechanical pin-coding.

Alternatively, the effects of incorrect insertion should be rendered non-hazardous by means of, for example, electrical coding of connector pins or allocation of unique addresses/identities.

The risk should be further reduced by means of warning labels and training of personnel.

(38) The screen should be robustly constructed and protected from excessive physical damage.

The electrical connection to the screen should be robust and securely fastened.

(39) Sufficiently robust insulation should be provided.

Clearance and creepage distances should fulfil at least the requirements for re-inforced insulation of EN 50124-1.

Protection should be provided against excessive physical damage.

Protection should be provided against electrically conductive foreign bodies.

(40) The fuse and its holder should be physically constructed and mounted so as to prevent the occurrence of a parallel short-circuit.

Means should be provided to prevent the use of an incorrectly rated fuse.

Means should be provided to prevent the use of a fuse with self-resetting or self-healing capability.

Table C.1 Resistors

(a) All kinds of resistor and adjustable resistor (excluding 4-terminal resistor)

Interruption	
Short-circuit	**(*)** Note 10
Increase of resistance value	
Decrease of resistance value	**(*)** Note 10
Short-circuit to case	

(b) Four-terminal resistor

Interruption of each terminal	
Interruption of resistance material	**(*)** Note 11
Short-circuit	**(*)** Note 10
Increase of resistance value of each terminal	
Decrease of resistance value	**(*)** Note 10
Short-circuit between two terminals of same side	**(*)** Note 12
Short-circuit to case	

Table C.2 Capacitors

(a) All kinds of capacitor and adjustable capacitor (excluding 4-terminal capacitor)

Interruption	
Short-circuit	**(*)** Note 14
Increase of capacitance	**(*)** Note 13
Decrease of capacitance	**(*)** Note 13
Decrease of parallel resistance	**(*)** Note 14
Increase of series resistance	
Short-circuit to case	

(b) Four-terminal capacitor

Interruption of each terminal		
Short-circuit		
Increase of capacitance	**(*)**	Note 13
Decrease of capacitance	**(*)**	Note 13
Decrease of parallel resistance	**(*)**	Note 14
Increase of series resistance		
Short-circuit between two terminals of same side	**(*)**	Note 12
Short-circuit to case		

Table C.3 Electromagnetic components

(a) Inductor

Interruption of winding		
Short-circuit of winding:		
- between turns	**(*)**	Note 15
- between layers	**(*)**	Note 16
- whole winding	**(*)**	Note 16
Short-circuit or decrease of insulation between winding and body	**(*)**	Note 16
Increase of resistance of winding		
Increase of inductance	**(*)**	Note 17
Decrease of inductance	**(*)**	Note 17

(b) Transformer

Interruption of any winding		
Short-circuit of any winding:		
- between turns	**(*)**	Note 15
- between layers	**(*)**	Note 16
- whole winding	**(*)**	Note 16
Short-circuit or decrease of insulation between windings	**(*)**	Note 16
Short-circuit or decrease of insulation between any winding and body	**(*)**	Note 16
Increase of resistance of any winding		
Increase of inductance of any winding	**(*)**	Note 17
Decrease of inductance of any winding	**(*)**	Note 17
Change of transfer ratio	**(*)**	Note 18

(c) Transductor (saturable reactor or magnetic amplifier)

Interruption of any winding		
Short-circuit of d.c. winding		
Short-circuit of a.c. winding:		
- between turns	**(*)**	Note 15
- between layers	**(*)**	Note 16
- whole winding	**(*)**	Note 16
Short-circuit or decrease of insulation resistance:		
- between d.c. and a.c. windings	**(*)**	Note 16
- between any winding and body	**(*)**	Note 16
Increase of inductance of a.c. winding	**(*)**	Note 17
Decrease of inductance of a.c. winding	**(*)**	Note 17
Increase of transductance	**(*)**	Note 19
Decrease of transductance		
Increase of d.c. threshold voltage		
Decrease of d.c. threshold voltage	**(*)**	Note 19

(d) Relay

Interruption of any coil		
Interruption of any contact		
Short-circuit or decrease of insulation resistance:		
- across open contacts	**(*)**	Note 20
- between coil and coil	**(*)**	Note 16
- between coil and contact	**(*)**	Note 20
- between coil and case	**(*)**	Note 16
- between contact and contact	**(*)**	Note 20
- between contact and case	**(*)**	Note 20
Welding of contacts	**(*)**	Note 21
Increase of contact resistance		
Contact chatter		
Increase of pick-up current		
Decrease of pick-up current	**(*)**	Note 22
Increase of drop-away current		
Decrease of drop-away current	**(*)**	Note 22
Change of pick-up to drop-away ratio	**(*)**	Note 22
Increase of pick-up time		
Decrease of pick-up time	**(*)**	Note 22
Increase of drop-away time	**(*)**	Note 22
Decrease of drop-away time	**(*)**	Note 22
Relay does not pick up		
Relay does not drop away	**(*)**	Note 22
Closure of any front contact at the same time as any back contact (transient or continuous)	**(*)**	Note 22
Non-correspondence between front contacts		
Non-correspondence between back contacts		

Table C.4 Diodes

(a) Normal diode (power, signal, switching)

Interruption	
Short-circuit	
Increase of reverse current	
Decrease of reverse breakdown voltage	
Increase of conducting-state voltage	
Decrease of conducting-state voltage	
Increase of threshold voltage	**(*)** Note 23
Decrease of threshold voltage	**(*)** Note 23
Short-circuit to case	

(b) Zener diode

Interruption	
Short-circuit	
Increase of Zener voltage	**(*)** Note 24
Decrease of Zener voltage	**(*)** Note 24
Change of differential resistance	
Increase of reverse current	
Increase of forward conducting-state voltage	
Decrease of forward conducting-state voltage	
Increase of forward threshold voltage	**(*)** Note 23
Decrease of forward threshold voltage	**(*)** Note 23
Short-circuit to case	

Table C.5 Transistors

(a) Bipolar transistor

Interruption: - of emitter (E) - and/or base (B) - and/or collector (C)		
Short circuit: - between E and B - between B and C - between E and C - between E and B and C		
Short-circuit between two connections and interruption of the third connection		
Short-circuit between casing and E or B or C		
Increase of DC and/or AC amplification	**(*)**	Note 25
Decrease of DC and/or AC amplification		
Increase of base-emitter conducting-state voltage		
Decrease of base-emitter conducting-state voltage		
Increase of threshold voltage V_{BE}	**(*)**	Note 23
Decrease of threshold voltage V_{BE}	**(*)**	Note 23
Decrease of break-down voltage V_{EB} or V_{CB} or V_{CE}		
Change of rise time, fall time, turn-on time, turn-off time		
Increase of residual current I_{CB}, I_{EB}, I_{CE}		
Change of saturation voltage V_{CE}		

(b) Field-effect transistor (FET)

Interruption: - of gate (G) - and/or source (S) - and/or drain (D)	
Short-circuit: - between S and D - between G and D - between S and G - between S and G and D	
Short-circuit between two connections and interruption of the third connection	
Short-circuit between casing and S or G or D	
Increase of forward transconductance	**(*)** Note 25
Decrease of forward transconductance	
Increase of gate threshold voltage	
Decrease of gate threshold voltage	
Decrease: - of drain-source break-down voltage - of gate-source and drain-gate maximum rated voltages	
Change of turn-on-time and turn-off time	
Increase of residual current I_{GS}, I_{DS}, I_{GD}	
Change of static drain to source on-state resistance	

Table C.6 Controlled rectifiers

(a) Silicon - controlled rectifier (SCR) (thyristor)

Interruption: - of gate (G) - and/or anode (A) - and/or cathode (C)	
Short-circuit: - between G and C - between G and A - between A and C - between A and G and C	
Short-circuit between two connections and interruption of the third connection	
Short-circuit between casing and A or G or C	
Change of holding current	
Change of gate trigger current and/or of gate trigger voltage	
Decrease: - of anode-cathode forward blocking voltage - of anode-cathode reverse blocking voltage - of reverse gate maximum rated voltage	
Change of turn-on time and turn-off time	
Increase of residual current I_{AC}, I_{GC}, I_{GA}	
Change of forward static on-voltage	

(b) Bidirectional thyristor (triac)

Interruption: - of gate (G) - and/or of MT1 (first current-carrying terminal) - and/or of MT2 (second current-carrying terminal)	
Short-circuit: - between G and MT1 - between G and MT2 - between MT1 and MT2 - between MT1 and G and MT2	
Short-circuit between two connections and interruption of the third connection	
Short-circuit between casing and MT1 or G or MT2	
Change of holding current	
Change of gate trigger current and/or of gate trigger voltage	
Decrease of MT1 - MT2 maximum rated off-state voltage and/or of gate maximum rated voltage	
Increase of residual current MT1-MT2, G-MT1, G-MT2	
Change of static on-voltage	

Table C.7 Surge Suppressors

(a) Voltage-dependent resistor (VDR) (varistor)

Interruption	
Short-circuit	
Increase of clamp voltage	
Decrease of clamp voltage	
Increase of residual current	

(b) Protective diode (tranzorb)

Interruption	
Short-circuit	
Increase of breakdown voltage	**(*)** Note 24
Decrease of breakdown voltage	**(*)** Note 24
Increase of residual current	
Short-circuit to case	

(c) Gas-discharge arrester

Interruption	
Short-circuit	
Increase of breakdown voltage	
Decrease of breakdown voltage	
Increase of leakage current	

(d) Air-gap arrester

Interruption	
Short-circuit	
Increase of breakdown voltage	
Decrease of breakdown voltage	
Increase of leakage current	

Table C.8 Opto-electronic components

(a) Photo diode

Interruption	
Short-circuit	
Increase of light sensitivity	**(*)** Note 25
Decrease of light sensitivity	
Increase of leakage current	

(b) Photo transistor

Interruption	
Short-circuit	
Increase of light sensitivity	**(*)** Note 25
Decrease of light sensitivity	
Increase of leakage current	

(c) Light-emitting diode (LED)

Interruption	
Short-circuit	
Increase of light emission (at constant current)	**(*)** Note 26
Decrease of light emission (at constant current)	
Increase of leakage current	
Increase of threshold voltage	**(*)** Note 23
Decrease of threshold voltage	**(*)** Note 23
Light emission below threshold voltage	**(*)** Note 26
Light emission with reverse polarity	**(*)** Note 27

(d) Optocoupler and self-contained fibre-optic system (see Note 28)

Short-circuit or decrease of insulation resistance: - between input and output - between adjacent systems in the same case	 **(*)** Note 29 **(*)** Note 29
Short-circuit to casing	
Change of switching time	
Increase of current transfer ratio	**(*)** Note 25 and 26
Decrease of current transfer ratio	

Table C.9 Filters

(a) Crystal

Interruption	
Short-circuit	
Change of resonant frequency	
Decrease of Q-factor	
Short-circuit to casing	

(b) Mechanical resonator (turning fork/reed/pendulum)

Interruption	
Short-circuit or decrease of insulation resistance:	
- between input and output	**(*)** Note 30
- between input or output and case	**(*)** Note 30
Change of resonant frequency	**(*)** Note 31
Increase of transfer ratio	**(*)** Notes 32 and 33
Decrease of transfer ratio	
Increase of Q-factor	**(*)** Note 33
Decrease of Q-factor	**(*)** Notes 31 and 34

Table C.10 Interconnection assemblies

(a) Printed-circuit board

Interruption or increase of resistance in one or more lines	
Short-circuit or decrease of insulation between two different lines	**(*)** Note 35

(b) Connector

Interruption of: - one or more contacts - shield		
Short-circuit or decrease of insulation resistance: - between contact and contact - between contact and shell	**(*)** **(*)**	Notes 35 and 36 Notes 35 and 36
Wrong mechanical position	**(*)**	Note 37

(c) Cable and wire

Interruption or increase of resistance in one or more wires		
Interruption or increase of resistance of screen	**(*)**	Note 38
Short-circuit or decrease of insulation resistance: - between wire and wire, or more than one wire, in any combination - between wire or wires and screen in any combination - between wire or wires or screen and external conductive parts	**(*)** **(*)** **(*)**	Note 39 Note 39 Note 39
Multiple interruptions and short-circuits	**(*)**	Note 39

(d) Connection - soldered, welded, wrapped, crimped, clipped, screwed

Interruption	
Increase of resistance	

(e) Fibre-optic cable

Interruption	
Increase of attenuation	

(f) Fibre-optic connector

Interruption	
Increase of attenuation	

Table C.11 Fuses

Interruption	
Parallel short-circuit	**(*)** Note 40
Increase of rupture current	**(*)** Note 40
Increase of rupture time	**(*)** Note 40
Reconnection after rupture	**(*)** Note 40

Table C.12 Switches and push/pull buttons

Interruption of any contact	
Short-circuit or decrease of insulation resistance: - across open contacts - between contact and contact - between contact and case	 **(*)** Note 20 **(*)** Note 20 **(*)** Note 20
Welding of contacts	**(*)** Note 21
Increase of contact resistance	
Device jammed in current state	
Contact chatter	

Table C.13 Lamps

Interruption	
Short-circuit	
Decrease of light intensity	
Short-circuit to case	

Table C.14 Batteries

Interruption	
Short-circuit: - of individual cell - of multiple cells - of whole battery	
Decrease of e.m.f.	
Increase of internal resistance	

Table C.15 Transducers/sensors (not including those with internal electronic circuitry

Interruption	
Short-circuit	
Output too high	
Output too low	
Time response too long	
Short-circuit to case	

Table C.16 Integrated circuits

(a) Analogue devices

Functional malfunction:	see annex C.3	

(b) Digital devices

Functional malfunction:	see annex C.3	

(c) Microprocessors

Functional malfunction:	see annex C.3	

D Annex D (Informative) Supplementary technical information

D.1 Introduction

This annex provides examples and guidance to supplement the technical requirements contained in sub-clause 5.4 and annex B of this standard. The given requirements are only valid for SIL3 or SIL4.

D.2 Achievement of physical internal independence

(Protection against influences of Type A, as referred to in annex B.3.2 of this standard)

D.2.1 Primary independence

The following measures provide "primary independence" between two items whose simultaneous malfunction could be hazardous:

1) Measures to avoid non-intentional galvanic connections

(Protection of internal galvanic insulation)

a) Between lines on the same layer of a printed-circuit board:

- Insulation distances (creepage distances and clearances) should be dimensioned at least according to the requirements for re-inforced insulation of EN 50124-1.

b) Between lines on different layers of a multilayer printed-circuit board:

c) Between insulated wires in the same cable:

d) Between insulated windings in the same transformer:

- Maximum temperature inside transformers should be limited (including fault conditions), to avoid carbonisation.

e) Between insulated items inside an opto-coupler:

- Maximum temperature inside opto-couplers should be limited (including fault conditions), to avoid carbonisation.

2) Measures to avoid non-intentional effects via intentional connections

(Protection of internal interfaces)

Interfaces should be protected by means of devices with inherent properties.

3) Measures to avoid non-intentional effects via electromagnetic coupling (Protection against internal cross-talk)

Cross-talk between electronic networks should be prevented as follows:

a) If different items are on the same printed-circuit board, they should be supplied by different power-supply networks. If not, then the impedance of the ground network should be sufficiently low to avoid cross-talk, even in the event of faults.

b) If different lines on the same board need to be protected against cross-talk occurring between them, the necessary separation distance depends on the used technology, the coupling length and the coupling mechanism. This distance should be demonstrated for the normal operational mode by theoretical calculations and/or by practical measurements.

c) If necessary to avoid coupling in the event of faults, additional measures (for example, shielding or doubling of distance) should be taken.

Effectiveness should be demonstrated by theoretical calculations and/or by practical measurements.

D.2.2 Secondary Independence

The following measures provide "secondary independence" between two items whose simultaneous malfunction could not be hazardous:

1) Each item in a n-out-of-m system may consist of a number of independent items.

2) Independence of two items whose simultaneous malfunction could be hazardous is achieved as written in annex D.2.1 (primary independence). These items will be referred to as "main items". Each main item can have one or more so called "additional items" checking the main item.

3) The degree of independence between a main item and an additional item may be less than written in annex D.2.1 and is called "secondary independence".

4) Main items are independent from additional items if all possible first-fault-effected influences between them are detected before they can become hazardous through further faults.

5) The following simplifications to annex D.2.1 are allowed for secondary independence:

- Insulation distances (creepage distances and clearances) should be dimensioned at least according to the requirements for basic insulation of EN 50124-1.
- Protecting devices do not require inherent properties. (Only a second fault may be able to inhibit the independence between a main item and an additional item).
- At least the power-supply network for the voltage-monitoring (additional item) should be separated from the power-supply network for the monitored main item as written in this paragraph.

D.3 Achievement of physical external independence

(Protection against influences of type C, as referred to in annex B.3.2 of this standard)

The following measures provide physical external independence:

1) Measures should be taken to avoid non-intentional effects by EMI/ESD disturbing correct operation, in accordance with EN 50121-4.

2) The specified climatic conditions should normally be complied with. Measures should be taken to minimise the risk of the system being operated outside its specified climatic conditions.

3) Measures to avoid non-intentional effects by mechanical stresses disturbing the correct operation:

a) Measures should be taken to ensure reliable correct operation in spite of mechanical stress-conditions agreed between the railway authority and supplier.

b) Protection should be compliant with EN 50125-1 and/or EN 50125-3 as appropriate.

4) Measures should be taken to ensure reliable correct operation in spite of chemical stress-conditions agreed between the railway authority and supplier.

5) Measures should be taken to avoid non-intentional operation under non-permitted power-supply voltages (protection of supply-voltages):

a) Non-permitted supply voltages (outside data-sheet values for supplied systems/equipments/components) should be disclosed by voltage-monitoring triggering a safe state before hazardous situations are possible.

b) Voltage-monitoring should operate correctly for the whole life-cycle. Voltage-monitoring redundancy may be necessary if disclosure of voltage-monitoring faults is not possible.

6) Measures should be taken to avoid non-intentional hazardous effects caused by external voltages across input and output ports disturbing the correct operation (protection of external interfaces):

a) Worst-case external voltages should be assumed (process-voltages and all possible EMI-induced voltages on cables and lines).

b) Clearances between live parts and exposed conductive parts/earth/circuits whose correct operation needs to be protected should be dimensioned according to surge voltages specified in EN 50124-1.

c) Creepage distances between live parts and exposed conductive parts/earth/circuits whose correct operation needs to be protected should be dimensioned according to EN 50124-1 and according to maximum rated r.m.s. voltages during operation.

d) For dimensioning insulation, the larger distance (clearance or creepage distance) is decisive.

D.4 Example of a method for single-fault analysis

(As referred to in annex B.3.3 of this standard)

NOTE 1: The information for the following paragraphs 1-6 are derived from CENELEC paper CLC/SC9XA(sec)114 : "Calculation with Mü8004 Formulas".

1) Depending on the sum "a" of the failure rates of the items whose simultaneous malfunctioning could be hazardous, the detection-plus-negation time t_{sf} of single faults in the respective items should not exceed the value:

$$t_{sf} \leq \frac{k}{1000 \cdot a}$$

k = 1 for a 2 out of 2 system;
k = 0.5 for a 2 out of 3 system.

2) The failure rates mentioned in paragraph (1) above are to be determined as a function of the stress profile dependent on the environmental conditions during operation. The stress profile depends on the application. A simplified stress profile may be taken as a basis if this has an unfavourable effect on the failure rate.

3) If within a system, sub-system or equipment comprising several items not all combinations of two failed items would be hazardous, the fault detection time may be determined separately for the various combinations. If, in this case, different fault detection times result for one item, the shortest time is decisive.

4) Periodic tests for faults in all items should be implemented. The tests should be representative for all credible faults affecting the correct operation, and should be finished within a time < t_{sf}.

Detection of faults in large-scale integrated circuits should be compliant with table D.1.

5) If a fault-free 2-out-of-n system (n = 2 or 3) is disconnected from the power supply, the fault detection may be interrupted. The duration of such a service interruption should not exceed the 400-fold value of the fault detection time which is permissible according to paragraph (1) above.

NOTE 2: This is based on the assumption that the reliability of electronic components is 20 times better when the equipment is not powered.

6) In the case of the fault detection being interrupted for a longer time than permissible according to paragraph (5) above, the system/sub-system/equipment may only be put into operation again after having been checked for multiple faults.

NOTE 3: The information for the following paragraphs 7-10 are derived from Italian Railway Technical Standard for Safety Electronic Systems (IS 353). This IS 353 complies with ORE A155.3 recommendation.

7) When the safety-related function is performed by a single item the disclosure time of a wrong side failure t_{sf} is the maximum total time to detect and react in a safe way to a single fault. The disclosure time shall not exceed the specified limit for the duration of any hazardous condition. In order to avoid any hazardous condition this duration must be less than the required response time of the equipment to be controlled (by means of the single item system).

8) The response time depends on the kind of the equipment to be controlled and therefore it is application dependent.

For example the t_{sf} could assume the following values:

t_{sf} < 100ms, if the equipment to be controlled is a signalling relay.

9) During the time t_{sf} the first safety related failure must be detected and it must trigger a safety reaction.

10) Periodic tests for faults should be implemented in the single item case. The tests should be representative for all faults affecting the correct operation, and should finish within a time < t_{sf}.

D.5 Example of a method for multiple-fault analysis

(As referred to in annex B.3.5 of this Standard)

NOTE: The information for the following paragraphs 1-2 are derived from CENELEC paper CLC/SC9XA(sec)114 : "Calculation with Mü8004 Formulas".

1) Double fault which could be hazardous if combined with a third fault:

a) If the timely detection-plus-negation of a fault in one item is impossible or unsuitable, the chance occurrence of a further fault in a second item should be taken into account.

b) It is necessary that simultaneous faults in two items are non-hazardous. This means that at least three independent items are necessary. They are connected such that only the malfunction of three items could be hazardous, as in a 3 out of 3-system.

c) Depending on the sum "a" of the failure rates of at least three items, whose simultaneous malfunction could be hazardous, the detection-plus-negation time t_{df} for double faults should not exceed the value:

$$t_{df} \leq \frac{2}{a}$$

d) The failure rates mentioned in c) should be determined as a function of the stress profile dependent on the environmental conditions during operation. The stress profile depends on the application. A simplified stress profile may be taken as a basis if this has an unfavourable effect on the failure rate.

e) If within a system, sub-system or equipment comprising several items not all combinations of three failed items would be hazardous, the fault detection time may be determined separately for the various combinations. If, in this case, different fault detection times result for two items, the shortest time is decisive.

2) Triple fault which could be hazardous if combined with a fourth fault:

a) If the timely detection-plus-negation of a double fault in two items is impossible or unsuitable, the chance occurrence of a further fault in a third item should be taken into account.

b) It is necessary that simultaneous faults in three items be non-hazardous. This means that at least four independent items are necessary. They are connected such that only the malfunction of four items could be hazardous, as in a 4 out of 4-system.

c) Measures for detection of triple faults, over and above the operational data flow and the tests during maintenance, are not required if the failure rate "a" does not exceed the value:

$$a \leq 2 \cdot 10^{-4} h^{-1}$$

d) The failure rate "a" is the sum of the failure rates of those items whose simultaneous malfunction could be hazardous (quadruple fault).

3) Coherently with the previous point D.4, Note 3 it must not be possible for further failures to cancel out a safe reaction. This could be allowable only in a controlled manner as part of corrective maintenance actions which must be executed when the faulty section of the item is off-line.

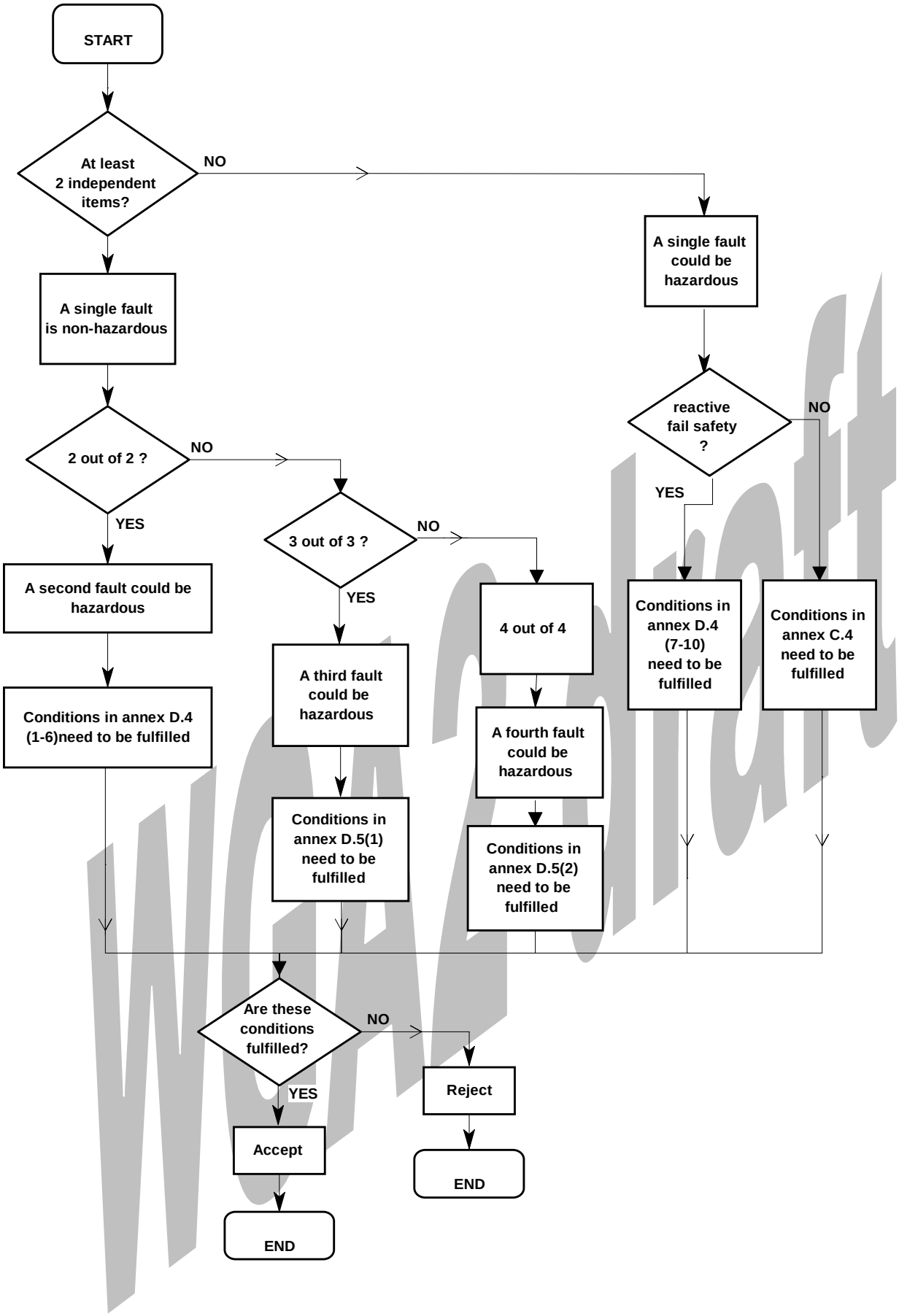


Figure D.1: Example of a fault analysis method

Table D.1: Examples of measures to detect faults in large-scale integrated circuits by means of periodic on-line testing, with comparison (SW or HW), in a 2-out-of-n system.

(Application-independent detection of a first fault before a second fault is to be assumed.)

COMPONENT	MALFUNCTION	MEASURES
1. CPU		
1.1 Register	Any, for example dependency on combinations of data bits (pattern - sensitive fault)	Using all registers (except initialisation registers) in all possible patterns (combinations of data bits); After initialising an initialisation register (e.g. interrupt control register), the correct initialised function needs to be tested; Registers greater than 8 bits may be tested by using all following combinations of data bits: ..5555....H 0AAAA....H ..3333....H 9999....H 0CCCC....H 6666....H 0000....H 0FFFF....H 0F0F0....H ..0F0F....H in each on-line test period. Additional on-line tests with all combinations of data bits are necessary, distributed over several test periods (using, for example, a random number generator).

COMPONENT	MALFUNCTION	MEASURES
1.2 Instruction decoding and execution	Any, for example wrong decoding or wrong execution affecting registers or memories, dependent on combinations of data bits at source and/or destination.	Using one instruction of each type, testing with combinations of data bits mentioned in 1.1; Test of whether all usable system-related instructions are executable, for all conditions, sources, destinations and values of address bits (loading program counter included); Test of whether all usable system-related Interrupt instructions are executable, dependent on interrupts or interrupt conditions; To test all usable system-related instructions, it is permissible to generate them in RAM and to jump to them for execution; After execution-related changing of the contents of at least one register, it is recommended to check not only the contents of concerned registers but also the contents of all other registers.
1.3 Clock	Wrong frequency	If independent clock generators are used for each computing channel, then wrong frequency in one channel can be detected by comparison; In cases of multiple faults, additional frequency monitoring may be necessary.
1.4 Reset	Additional or no reset(s)	If independent reset-generators are used for each computing channel, then a wrong reset in one channel can be detected by comparison; In cases of multiple faults, additional correct-start monitoring may be necessary.

COMPONENT	MALFUNCTION	MEASURES
1.5 Power Supply	Wrong supply voltage	If independent power supplies are used for each computing channel, then a wrong supply voltage in one channel can be detected by comparison; In cases of no independence, or multiple faults, additional voltage monitoring may be necessary.

2. Memory 2.1 ROM	Any wrong content(s) and any wrong decoding of address(es) or control signals(s).	Reading and comparing all contents.
2.2 RAM	Any wrong content(s) after reading or writing, and any wrong decoding of address(es) or control signal(s).	Reading and comparing all contents; Writing/reading/comparing test with all combinations of data bits mentioned in 1.1; Test whether all cells are addressable (e.g. by loading a particular combination of data bits into one cell and reading/comparing all other cells of the concerned chip). The same once more by loading the inverted particular combination of data bits into the same cell. All this to be repeated for the next cell in the same manner, and so on until all cells in all RAM chips are used; The last described test also detects influences from each bit to each other bit in the same RAM circuit. This test may be distributed over several on- line test periods.

E Annex E (Informative) Techniques and measures for safety-related electronic systems for signalling for the avoidance of systematic faults and the control of random and systematic faults

This annex relates architectures, techniques and measures to avoid systematic faults and control random and systematic faults on the level of systems/sub-systems/equipments within the safety management process to the different Safety Integrity Levels 1-4.

Therefore the following tables describe the various techniques/measures against the 4 SILs.

It is not possible to list all individual causes of systematic faults during the life-cycle phases, because systematic faults have different effects in the different life-cycle phases and measures are dependent on the application. A quantitative analysis for the avoidance of faults is therefore not possible.

According to the system life-cycle and the safety management process described in EN 50126 and referred in chapter 5.3 "Evidence of safety management" a number of activities shall be performed at each life-cycle phase. As described in the safety management process the purpose of the process is to reduce further the incidence of safety related human errors throughout the life-cycle and thus minimise the residual risk of safety related systematic faults. This includes verification and quality assurance processes. The requirements for this process are listed in:

Table E.1: Safety planning and quality assurance activities
(referred to chapter 5.2 and 5.3.4).

Following the phases 1 to 4 described in EN 50126

- Phase 1: Concept
- Phase 2: System definition and application conditions
- Phase 3: Risk analysis
- Phase 4: System requirements

the results shall be documented in the System Requirements Specification, which shall take account of the techniques/measures in

Table E.2: System requirements specification (referred to in chapter 5.3.6).

During the preparation of a Safety Plan the safety management structure shall be identified. Supporting information is given in:

Table E.3: Safety organisation
(referred to chapter 5.3.3).

During the life-cycle phase design and implementation (phase 6) the system architecture description shall be documented with consideration to:

Table E.4: Architecture of system/sub-system/equipment (referred to in section 5.4).

For the avoidance and control of faults caused by:

- Any residual design faults;
- Environmental conditions;
- Misuse or operating mistakes;
- Any residual faults in the software;
- Human factors.

Techniques/measures for design features are given in:

Table E.5: Design features (referred to in section 5.4).

According to the design features the analysis of effects of faults has to identify RAM and safety constraints on hardware and software using RAMS analysis and the failure modes in annex C.

Methods to identify and evaluate the effects of faults are given in:

Table E.6: Risk reduction at the level of system element (referred to in section 5.4).

Whatever the design method is, it shall have the following features:

- Clear and precise documentation;
- Clear and precise expression of functionality;
- Transparency, modularity and traceability;
- Technological and time-related information;
- Testability during verification and validation.

Techniques/measures are given in

Table E.7: Design and development of system/sub-system/equipment (referred to chapter 5.3.7).

The intended design shall be documented with reference to:

Table E.8: Design phase documentation (referred to in section 5.2).

and validated against the techniques/measures in:

Table E.9: Verification and validation of the system and product design (referred to chapter 5.3.9).

Using the Hazard Log, a validation test report shall be established including:

- The version of the test specification used;
- The version of element (HW and SW) used;
- The tools and equipment used;
- The result of each test;
- Any discrepancy between expected and actual results;
- The analysis made and the decision taken in the case of discrepancy.

The results of the design/development phase and of the safety case will lead to application, operation and maintenance procedures which shall be documented taking into account the techniques/measures in:

Table E.10: Application, operation and maintenance (referred to in chapter 5.3.12, and 5.4).

With each technique or measure in these tables there is a recommendation for each Safety Integrity Level (SIL) 1 to 4.

"HR" This symbol means that the measure or technique is Highly Recommended for this safety integrity level. If this technique or measure is not used the rationale behind not using it shall be detailed.

"R" This symbol means that the measure or technique is Recommended for this safety integrity level.

"-" This symbol means that the technique or measure has no recommendation for or against being used.

Table E.1: Safety planning and quality assurance activities (referred to in section 5.2 and 5.3.4)

Technique/ Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Checklists	R: checklist of activities and items to be produced		R: checklist of activities and items to be produced	
2. Audit of tasks	R		HR	
3. Inspection of issues of documentation	HR: documents agreed between railway/safety authority and industry		HR: all documents	
4. Review after change in the safety plan	HR			
5. Review of the safety plan after each safety life-cycle phase	HR			

Table E.2: System requirements specification (referred to in section 5.3.6)

Techniques/ Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Separation of Safety-Related Systems from Non Safety-Related Systems	R: well defined interfaces between Safety-Related Systems and Non Safety-Related Systems (SRS)		HR: well defined interfaces between Safety-Related Systems and Non Safety-Related Systems (SRS) and interface analysis	
2. Graphical description including for example block diagrams	HR		HR	
3. Structured Specification	HR: manual hierarchical separation into subtasks, description of the interfaces		HR: hierarchical separation using formalised methods, automatic consistency checks, refinement down to functional level	
4. Formal or semiformal methods			R: computer-aided	
5. Computer aided specification tools		R: tools without preference for one particular design method	R: model oriented procedures with hierarchical subdivision, description of all objects and their relationship, common data base, automatic consistency check	
6. Checklists	R: prepared checklists for all safety life-cycle phases, concentration on the main safety issues		R: prepared detailed checklists for all safety life-cycle phases	
7. Hazard Log	HR: Hazard Log to be established and maintained throughout the system life-cycle			
8. Inspection of the specification	R		HR	

Note 1: *Checklists* or *Computer aided specification tools* shall be used with another method since they usually state what to do (in order not to forget something), but cannot guarantee the quality of what is actually achieved.

Table E.3: Safety organisation (referred to in section 5.3.3)

Technique / Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Training of staff in safety organisation	HR: initial training in all relevant safety activities		HR: repetitive training or regular executing in all relevant safety activities	
2. Independence of roles	see figure 6: Arrangement for independence			
3. Qualification of staff in safety organisation (see note 1)	HR: technical education or sufficient experience		HR: higher technical education or extensive experience	

Note 1: Staff involved in safety activities shall be competent to perform those activities (see 5.3.3)

Table E.4: Architecture of system/sub-system/equipment (referred to in section 5.4)

Techniques / Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Separation of safety-related systems from non safety-related systems	R	R	HR	HR
2. single electronic structure with self tests and supervision	R	R	-	-
3. Dual electronic structure	R	R	-	-
4. Dual electronic structure based on composite fail-safety with fail-safe comparison	R	R	HR	HR
5. single electronic structure based on inherent fail-safety	R	R	HR	HR
6. single electronic structure based on reactive fail-safety	R	R	HR	HR
7. Diverse electronic structure with fail-safe comparison	R	R	HR	HR
8. Justification of the architecture by a quantitative reliability analysis of the hardware	HR	HR	HR	HR

Note 1: All techniques of the grey shaded group are alternatives, i.e. R means that at least one of these techniques is recommended

Table E.5: Design features (referred to in section 5.4)

Technique/ Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Protection against operating errors	R: plausibility checks on each input command		HR: plausibility checks on each input command	
2. Protection against sabotage			R: additional organisational measures are necessary	
3. Protection against single fault for discrete components (B.3.1)	R: all hazardous failure modes to be either detected and negated or demonstrated to be inherently safe such as a result of inherent physical properties (See Annex C). EN 50124-1 requirements for basic insulation		HR: all hazardous failure modes to be either detected and negated or demonstrated to be inherently safe such as a result of inherent physical properties (see annex C). EN 50124-1 requirements for reinforced insulation	
4. Protection against single fault for integrated circuits for digital electronic technology (B.3.1, C.3)	R: stuck-at fault model	R: DC-fault model	HR: permanent and transient malfunction model on item level (examples for malfunctions of integrated circuits are defined in Annex D, table D.1)	
5. Physical independence within the safety-related architecture (B.3.2 type A and C)	R: insulation distances should be dimensioned at least according to EN 50124-1 (basic insulation)		HR: insulation distances should be dimensioned to the reinforced value according to EN 50124-1 (reinforced insulation)	
6. Detection of single faults (B.3.3)	R: revealed by deviation from normal operation	R: dependent on the safety target the time for detection -plus-negation of a single fault should be within the safety target	HR: dependent on the safety target the time for detection-plus-negation of a single fault should be within the safety target	
7. Retention of safe state (B.3.4)	R: indication to the operator the safety-related functions associated with this faulty item should not be used or relied upon		HR: automatically shut down the faulty item, sub-system or system from the process or blocking all safety-related functions of this faulty item, sub-system or system	
8. Multiple faults B.3.4)	R: revealed by deviation from normal operation	R: dependent on the safety target the time for detection plus-negation of a multiple	HR: dependent on the safety target, the time for detection-plus-negation of a multiple fault should be within the safety target	
9. Dynamic fault detection	R: on line dynamic testing should be performed to check the proper operation of the safety-related system and provide an indication to the operator	HR: on line dynamic testing should be performed to check the proper operation of the safety- related system and provide an indication to the operator	HR: on line dynamic testing should be performed to check the proper operation of the safety-related system and automatically shut down the faulty item, sub-system or system from the process or blocking all safety related functions of this faulty item, sub-system or system	

10. Program sequence monitoring	R: temporal or logical monitoring of the program sequence plus indication to the operator	HR: temporal or logical monitoring of the program sequence plus indication to the operator	HR: temporal and logical monitoring of the program sequence at many checking points in the program and automatically shut down the faulty item, sub-system or system from the process or blocking all safety related functions of this faulty item, sub-system or system	
11. Measures against voltage breakdown, voltage variations, overvoltage, low voltage	HR: measures against voltage breakdown, voltage variations, overvoltage, low voltage		HR: extended measures against voltage breakdown, voltage variations, overvoltage, low voltage	
12. Measures against temperature increase	HR: temperature sensor detecting over-temperature		HR: it is to be investigated the necessity of a safety shut down	
13. Software architecture	see EN 50128		see EN 50128	
14. Protection against systematic faults			R: independent secondary protection	R[1)]:independent secondary protection

Note 1: For complex systems: HR.

Table E.6: Risk reduction at the level of system/sub-system/equipment
(Referred to in section 5.4)

Techniques / Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Preliminary Hazard Analysis	HR	HR	HR	HR
2. Fault Tree Analysis	R	R	HR	HR
3. FMECA	R	R	HR	HR
4. HAZOP	R	R	HR	HR
5. Cause-Consequence diagrams	R	R	HR	HR
6. Markov diagrams	R	R	R	R
7. Event Tree	R	R	R	R
8. Reliability Block Diagram	R	R	R	R
9. Zonal Analysis	R	R	R	R
10. Common Cause Failure Analysis	R	R	HR	HR
11. Historical Event Analysis	R	R	R	R

Note 1: PHA, should only be considered at the early stages of the development. When precise technical information is available, during the design, the other methods should be preferred.

Table E.7: Design and development of system/sub-system/equipment (referred to in section 5.3.7)

Technique/ Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Structured Design	HR: design hierarchically broken down		HR: design hierarchically broken down and fully traceable back to requirements specification including references between specification, design, circuit diagrams and application documentation	
2. Modularisation	R: modules of limited size, each module isolated	HR: modules of limited size each module isolated	HR: use of fully validated, easily comprehensible modules of limited size, each module functionally isolated	
3. Formal or semiformal methods			R: computer-aided	
4. Computer aided design tools		R: computer support for complex designs	R: use of tools which are proven in use or validated, general computer-aided development	
5. Environmental studies (EMC, vibration etc.)	R	R	HR	HR

Table E.8: Design phase documentation (referred to in section 5.2)

Techniques/ Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Graphical description of sub-systems	HR	HR	HR	HR
2. Description of interfaces	HR	HR	HR	HR
3. Environment (EMC, vibrations) studies	R	R	HR	HR
4. Modification procedure	HR	HR	HR	HR
5. Maintenance manual	HR	HR	HR	HR
6. Manufacturing documentation	HR	HR	HR	HR
7. Application Documentation	HR	HR	HR	HR

Table E.9: Verification and validation of the system and product design
(referred to in section 5.3.9)

Technique/ Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Checklists	R: prepared checklists, concentration on the main safety issues		R: prepared detailed checklists	
2. Simulation		R	R	
3. Functional testing of the system	HR: functional tests, reviews should be carried out to demonstrate that the specified characteristics and safety requirements have been achieved		HR: comprehensive functional tests should be carried out on the bases of well defined test cases to demonstrate the specified characteristics and safety-requirements are fulfilled	
4. Functional testing under environmental conditions	HR: the testing of safety-related functions and other functions under the specified environmental conditions should be carried out		HR: the testing of safety-related functions and other testing under the specified environmental conditions should be carried out	
5. Surge immunity testing	HR: surge immunity should be tested to the boundary values of the real operational conditions	HR: surge immunity should be tested higher / higher limit than the boundary values of the real operation conditions		
6. Calculation of failure rates	HR: on the basis of typical conditions		HR: on the basis of worst case conditions	
7. Inspection of documentation	HR			
8 Ensure design assumptions are not compromised by manufacturing process			HR: specify manufacturing requirements and precautions, plus audit of actual manufacturing process by safety organisation	
9. Test facilities	R: designer of the test facilities should be independent from the designer of the system or product		HR: designer of the test facilities should be independent from the designer of the system or product	
10. Design review	HR: reviews should be carried out at appropriate stages in the life-cycle to confirm that the specified characteristics and safety requirements have been achieved		HR: reviews should be carried out at appropriate stages in the life-cycle to confirm that the specified characteristics and safety requirements have been achieved	
11. Ensure design assumptions are not compromised by installation and maintenance processes	HR: specify installation and maintenance requirements and precautions		HR: specify installation and maintenance requirements and precautions, plus audit of actual installation and maintenance processes by safety organisation	
12 High confidence demonstrated by use (optional)	R: 10000 hours operation time, at least 1 year experience with equipments in operation		R: 1 million hours operation time, at least 2 years experience with different equipments including safety analysis, detailed documentation also of minor changes during operation time	

Note 1: Checklists, Computer aided specification tools and Inspection of the specification can be used in the verification activity of a phase.

Table E.10: Application, operation and maintenance (referred to in sections 5.3.12, and 5.4)

Technique/ Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Production of applications operational and maintenance instructions	R: all operational, application and maintenance instructions traceable back to the design including use of hazard log		HR: all operational, application and maintenance instructions traceable back to the design including use of hazard log	
2. Training in the execution of operational and maintenance instructions (see 5.4, section 5)	HR: initial training of all operators and maintenance staff		HR: initial training plus periodic refresher training of all operators and maintenance staff	
3. Operator friendliness	HR: the interaction between the person and the system to be as simple as possible, in order to reduce the risk of human errors			
4. maintenance friendliness	HR: separate diagnosis tools, safety-related maintenance measures as seldom as possible		HR: sufficient, sensible and simply handled diagnosis tools shall be included for unavoidable repairing measures, safety-related maintenance measures as seldom as possible or not necessary at all	
5. Protection against operating errors	R: procedural plausibility checks on each input command		HR: procedural plausibility checks on each input command	
6. Protection against sabotage			R: additional organisational measures are necessary	

F Annex F (Informative) Bibliography

The following documents were consulted during the preparation of this standard (in addition to the Normative References listed in Section 3) :

IEC 812:1985	Analysis techniques for system reliability - Procedure for failure modes and effects analysis (FMEA)
UIC/ORE report A155/RP6	Computer-based safety systems requirements specification, September 1985
UIC/ORE report A155/RP7	The design of computer-based safety systems, April 1986
UK Health & Safety Executive	Programmable electronic systems in safety-related applications - Parts 1 and 2, 1987
UIC/ORE report A155/RP11	Proof-of-Safety of computer-based safety systems, September 1987
UIC/ORE report A155/RP12	Failure catalogue for electronic components, April 1988
MIL-HDBK-338-1A	Electronic reliability design handbook, October 1988
IEC 1025:1990	Fault Tree Analysis (FTA)
German Federal Railways Mü8004	Principles for the technical approval of signalling and communications technology, January 1991
Reliability Analysis Center report FMD-91	Failure mode/mechanism distributions, September 1991
IRSE International Technical Committee report No.1	Safety system validation with regard to cross-acceptance of signalling systems by the railways, January 1992
CLC/SC9XA(sec)114	Calculation with Mü8004 formulas, August 1994
ISO 9001:1994	Quality Systems - Model for quality assurance in design, development, production, installation and servicing
IEC 61508	Functional safety of electrical/electronic/ programmable electronic safety-related systems
CLC R009-001	Hazardous failure rates and Safety Integrity Levels, CENELEC report
CLC R009-004	Systematic Allocation of Safety Integrity Requirements, CENELEC report